

NETCOMM GATEWAY SERIES
ADSL2+/3G Wireless N300
4-Port Modem Router

NetComm[®]



USER GUIDE

Preface

This manual provides information related to the installation, operation, and application of this device. The individual reading this manual is presumed to have a basic understanding of telecommunications terminology and concepts.

If you find the product to be broken or malfunctioning, please contact technical support for immediate service by email at technicalsupport@netcomm.com.au

For product update, new product release, manual revision, or software upgrades, please visit our website at <http://www.Netcomm.com.au>

Important Safety Instructions

With reference to unpacking, installation, use and maintenance of your electronic device, the following basic guidelines are recommended:

- Do not use or install this product near water, to avoid fire or shock hazard. For example, near a bathtub, kitchen sink or laundry tub, or near a swimming pool. Also, do not expose the equipment to rain or damp areas (e.g. a wet basement).
- Do not connect the power supply cord on elevated surfaces. Allow it to lie freely. There should be no obstructions in its path and no heavy items should be placed on the cord. In addition, do not walk on, step on or mistreat the cord.
- Use only the power cord and adapter that are shipped with this device.
- To safeguard the equipment against overheating, make sure that all openings in the unit that offer exposure to air are not blocked.
- Avoid using a telephone (other than a cordless type) during an electrical storm. There may be a remote risk of electric shock from lightning. Also, do not use the telephone to report a gas leak in the vicinity of the leak.
- Never install telephone wiring during stormy weather conditions.



WARNING

- Disconnect the power line from the device before servicing.

Copyright

Copyright©2008 NetComm Limited. All rights reserved. The information contained herein is proprietary to NetComm Limited. No part of this document may be translated, transcribed, reproduced, in any form, or by any means without prior written consent of NetComm Limited

NOTE:This document is subject to change without notice.

Save Our Environment

When this equipment has reached the end of its useful life, it must be taken to a recycling centre and processed separate from domestic waste.

The cardboard box, the plastic contained in the packaging, and the parts that make up this router can be recycled in accordance with regionally established regulations. Never dispose of this electronic equipment along with your household waste. You may be subject to penalties or sanctions under the law. Instead, ask for disposal instructions from your municipal government.

Please be responsible and protect our environment.

Table of Contents

Introduction	5
Your 3G15Wn – ADSL2+/3G Wireless N300 4-Port Modem Router	6
Package contents	6
Key features	6
Placement of your 3G15Wn	7
Router placement	8
Avoid obstacles and interference	8
Cordless phones	8
Choose the “quietest” channel for your wireless network	9
Product Layout	10
Getting to know your 3G15Wn	11
Minimum system requirements	12
Do I need a Microfilter?	12
Default settings	13
Restore factory default Settings	13
Connecting the 3G15Wn	13
Quick ADSL setup	14
Quick 3G setup	15
Establish a wireless connection	15
Advanced Configuration	16
What can you do from here	17
Logging into the user interface	17
Web User Interface	18
What can you do from here	19
Logg on to the web user interface	19
Basic	20
Quick Setup	21
Home	21
3G Settings	23
3G Interface	24
3G WAN Service	24
PIN Configuration	24
3G Backup Config	25
3G	25
Wireless	26
Setup/Basic	27
Security	28
Configuration	28
MAC filter	30
Wireless bridge	31
Station info	31
Management	32
Device Settings	33
Backup	33
Update	33
Restore Default	33
Update Firmware	34
SNMP	34
TR-069 client	35
SNTP	36
Access Control	36
Services	36
Passwords	36
Save/Reboot	37
Advanced	38
ATM interface	39
WAN service	39
LAN	40
NAT	41
Port Forwarding	41
Port Triggering	41
Security	43
IP Filtering	43
Parental Control	45
Time Restriction	45

URL filter.....	45
Quality of Service	46
Queue configuration.....	46
QoS classification	47
Routing	48
Default gateway	48
Static route	48
Policy routing.....	49
Dynamic router	49
DNS.....	50
DNS server	50
Dynamic DNS	50
DSL.....	50
UPnP	51
DNS proxy	51
USB Storage.....	52
Print Server.....	52
Interface grouping	53
LAN ports	53
Status	54
Diagnostics	55
System Log.....	56
Statistics	57
LAN	57
WAN.....	57
ATM.....	58
ADSL.....	58
Route.....	60
ARP	60
DHCP	60
Appendix A – Print Server.....	62
Appendix B – USB Storage.....	68
Legal and regulatory information.....	70

INTRODUCTION

Introduction

Your 3G15Wn – ADSL2+/3G Wireless N300 4-Port Modem Router



Congratulations on your purchase of a NetComm 3G15Wn – ADSL2+/3G Wireless N300 4-Port Modem Router. This product is a high-performance ADSL2+ Modem Router combined with a 3G router that provides high-speed wireless N networking and Internet connectivity for your home, office or public space. The NetComm 3G15Wn gives you the option to plug directly into an ADSL service to deliver Internet to users or connect via 3G with its support for an external 3G USB Modem. The choice is yours. Both methods will allow you to share your Internet connection amongst multiple users with either the 4 LAN ports for wired connections or via high-speed Wireless N.

The 3G15Wn also allows for a 3G Mobile Broadband connection provided by a 3G USB modem to act as a backup Internet connection to your fixed line service, providing automatic Internet failover to 3G in the event that the ADSL service fails. Should you have access to both connection methods, the 3G15Wn will ensure you are “always on” which is vital to some individuals and business that perform Internet critical operations.

The USB port not only has the capability to support an external 3G USB Modem, but it is also able to be used for the purpose of print and mass storage server. By simply plugging in a USB printer or a USB hard drive to the router, the functionality of these products will be able to be shared with everyone connected to the 3G15Wn.

The 3G15Wn features the latest standards of wireless security, with wireless security enabled by default on each router. An advanced firewall and VPN pass-through functionality allows for maximum security and caters for the encrypted Point-to-Point communications from connected computers through the 3G15Wn to a VPN Server.

The Port Forwarding and UPnP functionality provided by the 3G15Wn make it easier for today’s Internet users to setup and configure the various Network Port Rules needed by Internet applications such as On-Line Gaming, Peer-To-Peer file sharing and Instant Messaging services

Package contents

Your 3G15Wn contains the following items:

- 3G15Wn – ADSL2+/3G Wireless N300 4-Port Modem Router
- 12VDC, 1.5A Power Supply
- RJ-11 ADSL Line connection cable
- RJ-45 Ethernet cable
- Removable Antenna
- User Guide (on CD)
- Printed Quick Start Guide

Key features

- Fully featured ADSL2+ Modem Router
- USB port for alternative connection to the Internet via a 3G USB Modem
- Supports auto Internet failover from ADSL to 3G
- Wireless N access point – high speed wireless up to 300Mbps
- 2 Transmit and 2 Receive antennas
- 4 LAN ports for multiple wired connections
- Browser based interface for configuration and management: OS independent and easy to use
- Full wireless security - WEP, WPA, WPA2

PLACEMENT

Placement

Placement of your 3G15Wn

When Connecting With 3G

Just like your mobile phone, a 3G USB Modem's location will affect its signal strength to the 3G Mobile Base Station (Cell Tower). The data speed achievable from a 3G USB modem is relative to this signal strength, which is affected by many environmental factors. Please keep in mind that the 3G USB Modem will need adequate signal strength in order to provide Internet connectivity whilst choosing a location to place your 3G15Wn – ADSL2+/3G Wireless N300 4-Port Modem Router.

Similarly to the 3G USB Modem, the wireless connection between the Router and your Wi-Fi devices will be stronger the closer your connected devices are to your Router. Your wireless connection and performance will degrade as the distance between your Router and connected devices increases. This may or may not be directly noticeable, and is greatly affected by the individual installation environment.

If you have concerns about your network's performance that might be related to range or obstruction factors, try moving the computer to a position between three to five meters from the Router in order to see if distance is the problem. If difficulties persist even at close range, please contact NetComm Technical Support.

Note: While some of the items listed below can affect network performance, they will not prohibit your wireless network from functioning; if you are concerned that your network is not operating at its maximum effectiveness, this checklist may help.

Router placement

Place your Router as close as possible to the centre of your wireless network devices. To achieve the best wireless network coverage for your "wireless clients" (i.e., computers with built in or USB Wireless Adapters, Laptops with Built-in Wireless, Wireless PDA / iPhone, etc):

- Ensure that your Router's antennas are parallel to each other, and are positioned vertically (toward the ceiling). If your Router itself is positioned vertically, point the antennas in an upward direction as much as possible.
- In multi-storey homes, place the Router on a floor that is as close to the centre of the home as possible. This may mean placing the Router on an upper floor.
- Try not to place the Router near a cordless telephone that operates at the same radio frequency as the 3G15Wn (2.4GHz).

Avoid obstacles and interference

Avoid placing your Router near devices that may emit radio "noise," such as microwave ovens. Dense objects that can inhibit wireless communication include:

- Refrigerators
- Washers and/or dryers
- Metal cabinets
- Large aquariums
- Metallic-based, UV-tinted windows

If your wireless signal seems weak in some spots, make sure that objects such as these are not blocking the signal's path (between your devices and Router).

Cordless phones

If the performance of your wireless network is impaired after considering the above issues, and you have a cordless phone:

- Try moving cordless phones away from your Router and your wireless-enabled computers.
- Unplug and remove the battery from any cordless phone that operates on the 2.4GHz band (check manufacturer's information). If this fixes the problem, your phone may be interfering with the Wi-Fi Router.
- If your phone supports channel selection, change the channel on the phone to the farthest channel from your wireless network. For example, change the phone to channel 1 and move your Router to channel 11. See your phones user manual for detailed instructions.
- If necessary, consider switching to a 900MHz or 5GHz cordless phone.

Choose the “quietest” channel for your wireless network

In locations where homes or offices are close together, such as apartment buildings or office complexes, there may be wireless networks nearby that can conflict with your wireless network.

Use the Site Survey capabilities found in the Wireless Utility of your wireless adapter to locate any other wireless networks that are available (see your wireless adapter's user manual), and switch your Router and computers to a channel as far away from other networks as possible.

- Experiment with more than one of the available channels, in order to find the clearest connection and avoid interference from neighbouring cordless phones or other wireless devices.
- For NetComm wireless networking products, use the detailed Site Survey and wireless channel information included with your wireless network card. See your network card's user guide for more information.

These guidelines should allow you to cover the maximum possible area with your Router. Should you need to cover an even wider area, you should consider looking at building a hybrid network by combining your wireless network with a HomePlug Network. See the NetComm website for more details on HomePlug products

Product Layout

Product Layout

Getting to know your 3G15Wn

It is recommended that you take a moment to acquaint yourself with the indicator lights, ports and default settings of the 3G15Wn prior to commencing with installation.



LED	Colour	Mode	Function
Power	Green	On	The router is powered on
		Off	The router is not powered
LAN 1-4	Green	On	Ethernet link is established
		Off	There is no Ethernet link established
		Blinking	Data transmitting/receiving over Ethernet
Wi-Fi	Green	On	Wireless module is ready
		Off	Wireless Module is not installed
		Blinking	Data transmitting/receiving over Wi-Fi
ADSL	Green	On	The ADSL link is established
		Off	The is no ADSL link established
		Blinking	The ADSL line is training if it is blinking rapidly, The ADSL line is not connected if it is blinking slowly.
Internet	Red	On	Device attempted to obtain an IP address and failed (no DHCP response, no PPPoE response, PPPoE authentication failed, no IP address from IPCP etc.) For bridged mode, this LED remains off. If the IP or PPPoE session is dropped due to an idle timeout, the LED will remain green if an ADSL connection is still present. If the session is dropped for any other reason, the LED is turned off. The LED will turn red when it attempts to reconnect and DHCP or PPPoE fails
		Off	Modem is in bridged mode or ADSL connection is not present
	Green	Blinking	IP connected and data is passing through the device (either direction)
USB	Green	On	A USB device is plugged into the USB port
		Off	There is no USB device plugged into the USB port

Port Name	Function
Power	Connect the supplied power adapter
On/Off	Push to turn the 3G15Wn on and off
USB	Connect your external 3G USB Modem for a 3G connection or USB Storage/USB Printer
Reset	Reset button. Depress for 10 seconds to return your 3G15Wn to factory default settings
LAN x 4	4 x 10/100 Ethernet switch to connect wired devices
DSL	Telephone jack (RJ-11) to connect to your telephone wall socket (ADSL Line)
Wi-Fi	Wi-Fi antenna for distributing wireless Internet signal



Minimum system requirements

Different aspects of the 3G15Wn have different requirements, so let's look at them in turn. We'll start with your computer, which ought to match the following requirements if you are to enjoy the benefits of a high-speed ADSL connection and use of 3G and Wireless Networking.

PC Requirements:

- Any computer running Windows 98/2000/Me/XP/Vista/7 or Macintosh OSX
- Ethernet or Wireless Network card
- CD-ROM drive
- Web browser e.g.
 - Internet Explorer 5.1 (or better)
 - Netscape Navigator
 - Mozilla FireFox 1.0.4 (or better)

ADSL Requirement:

- ADSL broadband connection to an ISP (Internet Service Provider)
- ADSL In-line Splitter/Filter (Please refer to "Do I need a micro filter?" for more information)

Note: Connection at ADSL2 or 2+ rates depends on the service offered by your ISP; the device will operate at standard ADSL rates in the absence of the 2 or 2+ service. Consult your ISP for details.

3G Requirement:

- Compatible 3G USB Modem with Active SIM/Data Service if you want to use 3G Broadband service.

Note: Subject to terms and conditions from your 3G Mobile Broadband Service Provider.

Wireless Computer/Device Requirements

- Computer/device with a working 802.11b, 802.11g or 802.11n wireless adapter.

Do I need a micro filter?

Micro filters are used to prevent interference between phones and fax machines, and your ADSL service. If your ADSL-enabled phone line is being used with any equipment other than your ADSL Modem then you will need to use one Micro filter for each phone device in use. Telephones and/or facsimiles in other rooms that are using the same line will also require Microfilters. A suitable Microfilter can be purchased from NetComm or your Service Provider, if required.



Default settings

LAN (Management)

Static IP Address:	192.168.1.1
Subnet Mask:	255.255.255.0
Default Gateway:	192.168.1.1

WAN (Internet)

WAN mode:	DHCP
-----------	------

Wireless

SSID:	NetComm Wireless
Channel:	auto
Security:	WEP, 64bit
WEP Key:	a1b2c3d4e5

Interface Access

Username:	admin
Password:	admin

Restore Factory Default Settings

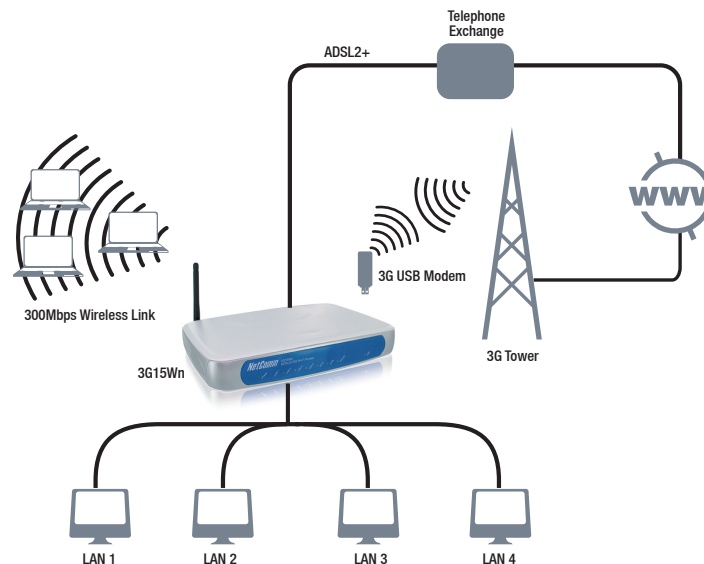
Restoring factory defaults will reset the 3G15Wn to its factory default configuration. Occasions may present themselves where you need to restore the factory defaults on your 3G15Wn such as:

- You have lost your username and password and are unable to login to your 3G15Wn's web configuration page;
- You have purchased your 3G15Wn from someone else and need to reconfigure the device to work with your ISP;
- You are asked to perform a factory reset by NetComm Support staff

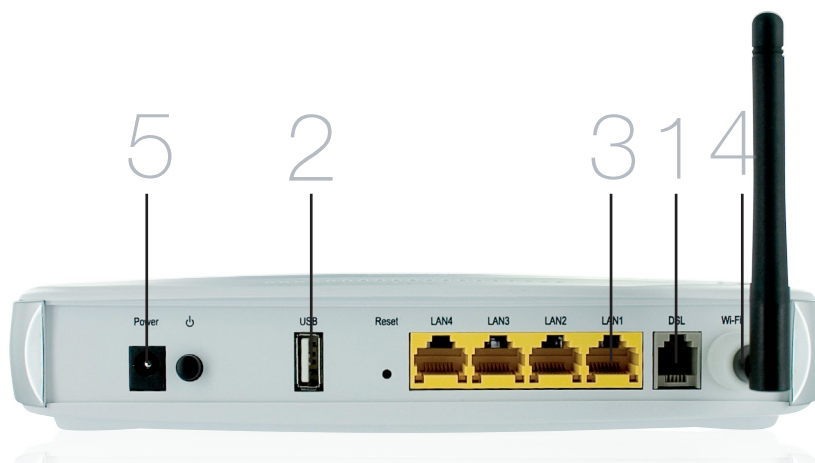
In order to restore your 3G15Wn to its factory default settings, please follow these steps:

- Ensure that your 3G15Wn is powered on (for at least 10 seconds);
- Use a paper clip or a pencil tip to depress the reset button for ten seconds and release. At this point, the reset is in progress. Do not power off the unit at this point;
- When indicator lights return to steady green, reset is complete. The default settings are now restored. The entire process takes about 45 seconds to complete;
- Once you have reset your 3G15Wn to its default settings you will be able to access the device's configuration web interface using <http://192.168.1.1> with username 'admin' and password 'admin';

Connecting the 3G15Wn



Quick Setup



1. Connect the supplied RJ-11 cable to the **DSL** port on the back of your router to the phone port that supplies your ADSL.
2. And/or, attach a compatible 3G USB modem into the **USB** port on the back of the router
3. Connect the supplied RJ-45 Ethernet cable from one of the **LAN** ports on the back of the router to your computer
4. Screw the supplied detachable antenna to the **Wi-Fi** connector on the back of the router
5. Connect the supplied power adapter to your router and press the on/off button to power the router on.

Login to the web interface

- Open a web browser (Internet Explorer, Firefox, and Safari) and type 192.168.1.1 into the address bar.
- At the login screen type admin into both the username and password fields. Then click submit. This will take you directly to the Quick Setup page

Basic > Quick Setup

- ADSL only
- 3G only
- ADSL with 3G backup

Next

Connecting With ADSL

Protocol: **PPPoE**

User ID:

Password:

VPI:

VCI:

1. Select the **ADSL only** box and click **Next**
2. Enter the **user ID/Password** on this screen as supplied by your ISP
3. Click on **Next** to use these settings
4. You will then be asked to enter additional setup details.

Connecting with 3G

Basic > Quick Setup > 3G Only

Network : 3Telstra
3G USB Dongle: ZTE INCORPORATED MF633+

Profile:

Authentication Method:

APN:

Username:

Password:

1. Select the **3G only** box and click **Next**
2. Your modem will auto detect if it is compatible: This information can be seen at the top of the page
3. From the drop down **Profile** box select your 3G ISP, which will auto-fill your APN setting
4. Enter the **username/password** supplied by your 3G ISP.

Note: Not all 3G users will have a username/password. Only enter this information if you have been supplied one by your 3G ISP

5. Click on **Next** to use these settings
6. You will then be asked to enter additional setup details. This will be explained from **Wireless Quick Setup**

Configuring 3G backup

Enable 3G Backup

Check Interval(sec.):

Retry times:

IP Address:

1. Select the **ADSL with 3G backup** box and click **Next**
2. Follow the instructions listed above for both ADSL and 3G to set up both connections
3. Check the **Enable 3G Backup** box and enter your desired backup settings
4. Click on **Next** to use these settings
5. You will then be asked to enter additional setup details. This will be explained from **Wireless Quick Setup**

Wireless Quick Setup

Enable Wireless

SSID:

Select Wireless Security level:

None WEP WPA

Network Authentication:

WEP Encryption:

Encryption Strength:

Current Network Key:

Network Key 1:

Network Key 2:

Network Key 3:

Network Key 4:

Enter 13 ASCII characters or 26 hexadecimal digits for 128-bit encryption keys
Enter 5 ASCII characters or 10 hexadecimal digits for 64-bit encryption keys

1. All the default settings already appear on the wireless quick setup page
2. You can enable/disable your wireless
3. You can change your wireless SSID. If you do, be sure to remember the new name or write it down so you know what network to connect to
4. You can also select the level of wireless security and change the wireless password
5. Once you have completed entering your wireless settings click **Next**

USB Storage

USB Status: detected

This page allows you to enable USB storage .

Enable USB storage.

Netbios Name:

Directory Name:

1. If a USB device is plugged into the USB port, it will be detected and you will have the choice to **Enable USB storage**
2. If you enable USB storage you will be shown the **netbios** and **Directory** name, you can change these to anything you want
3. Click **Next** once you are happy with the settings
4. To access the storage device open a web browser and type `\\Netbios\Directory\`. So using the defaults `\\3G15Wn\USB-Storage\`

USB Print Server

Enable on-board print server.

Printer name:

Make and model:

1. If a USB device is plugged into the USB port, it will be detected and you will have the choice to **Enable on-board print server**
2. If you enable the device to work as a print server you will be asked to enter the **printer name** and **make and model**. Both fields can be named anything you like. The names will be used to identify the printer later.
3. Click **Next** once you are happy with the settings
4. To complete setting up your network printer, please read **Appendix A** of the **User Manual**

Passwords

Access to your router is controlled through three user accounts: admin, support, and user.

The user name "admin" has unrestricted access to change and view configuration of your router.

The user name "support" is used to allow an ISP technician to access your router for maintenance and to run diagnostics.

The user name "user" can access the router, view configuration settings and statistics, as well as, update the router's software.

Use the fields below to enter up to 16 characters and click "Apply/Save" to change or create passwords. Note: Password cannot contain a space.

Username:

Old Password:

New Password:

Confirm Password:

1. On this page you can change the passwords for the different levels of users
2. The default password for all users is the same as the corresponding username
3. Once you have completed setting the passwords click **Finish**
4. You will be taken back to the home page where you can view your connection status

Establishing a Wireless Connection

You can connect multiple wireless devices, including laptops, desktops and PDA's to your device by following these two basic steps.

1. Using your wireless device, scan the wireless networks in your area and select the network called **NetComm Wireless**, then click **connect**.

Note: If you changed the SSID in the wireless quick setup, then your network name will be different

2. Enter the following default security key: **a1b2c3d4e5**

Note: If you are unable to connect, please refer to the user manual for details on how to connect to the wireless network.

Troubleshooting

Cannot establish a wireless connection

- Make sure the wireless switch on your laptop is in the **on** position
- Ensure your device and wireless adapter are using the same wireless security settings
- Make sure you are trying to connect to the correct SSID with the correct security key

Cannot establish an ADSL connection

- Ensure you have entered the correct **username** and **password** as supplied by your ISP. If you cannot find them please contact your ISP to ensure you have the correct details.

Cannot establish a 3G Connection

- Ensure you are using a compatible 3G USB Modem

Note: See NetComm Website for a list of compatible modems - www.netcomm.com.au

- Ensure you have entered the correct **3G Profile** (ISP name and pre/post paid) and that the **APN** is the same as supplied by your 3G ISP

Cannot access the Web UI

- If you have changed your username/password and forgotten them you will need to reset your router to the factory default settings and use the default settings **admin/admin**

How to reset your router to the factory default settings

- With a paperclip, sharp pencil or similar object press the **reset** button on the back panel of the device and hold for approximately 10 seconds.

Web User Interface

Web User Interface

What can you do from here?

By logging into the web user interface, you are able to configure your 3G15Wn with a wide array of basic and advanced settings. From setting wireless security, to backing up your routers settings, uploading new firmware and setting parental controls, the web user interface is a handy tool for personalizing your device to maximize its potential. See below, in the rest of this user manual for a more advanced description on all elements of the web user interface

Logging into the user interface

To login to the web interface, follow the steps below:

NOTE: The default settings can be found in Default Settings, listed earlier in this manual.

- 1: Open a web browser and enter the default IP address for the Router in the web address field. In this case **http://192.168.1.1**

NOTE: For local administration (i.e. LAN access), the PC running the browser must be attached to the Ethernet, and not necessarily to the device. For remote access, use the WAN IP address shown on the WUI Homepage screen and login with remote username and password.

- 2: A dialog box will appear, as illustrated below. Enter the default username and password, as defined in the section Default Settings.

Click OK to continue.



Username:	admin
Password:	admin

NOTE: The login password can be changed later (see Access Control > Passwords)

- 3: After successfully logging in for the first time, you will reach this following "Quick Setup" page.

Basic

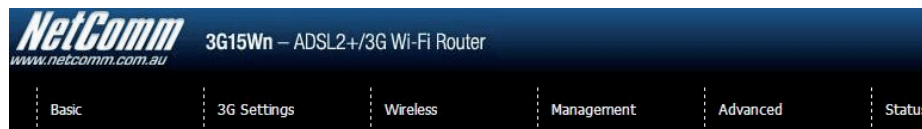
Basic

Quick Setup

After you log into the web user interface, you will be taken directly to the Quick Setup page. See the instructions listed above in “Quick Setup” for instruction on how to configure your device for use.



Home



Basic > Home

Model Name:	3G15Wn
Board ID:	96358A-2331N
Software Version:	J411-402NCM-T01_R01_20090915
ADSL Driver Version:	A2pB025c1.d22
Bootloader (CFE) Version:	1.0.37-102.6-8
Wireless Driver Version:	5.10.85.0.cpe4.402.4

Device Info for 3G

Network:	vodafone AU
Link:	Connecting
USB Vendor:	huawei
USB Model:	E220
Signal Strength:	
SIM Info:	READY
3G Backup:	Disable
3G Backup Interface:	None

This information reflects the current status of your connection.

Line Rate - Upstream (Kbps):	
Line Rate - Downstream (Kbps):	
LAN IPv4 Address:	192.168.1.1
WAN IP Address:	
Default Gateway:	ppp0
Primary DNS Server:	
Secondary DNS Server:	
Date/Time:	Sat Jan 1 00:44:10 2000

The web user interface (WUI) is divided into two window panels, the main menu (on the top) and the display screen (on the bottom). The main menu has the following options: Basic, 3G Settings, Wireless, Management, Advanced and Status.

Selecting one of these options will open a submenu with more options. Basic is discussed below while subsequent chapters introduce the other main menu selections.

NOTE: The menu options available within the web user interface are based upon the device configuration and user privileges (i.e. local or remote).

The following table provides further details:

Field	Description
Model Name	Model number of your device
Board ID	The unique number of the board inside your device
Software Version	The current version of software loaded on your device
ADSL Driver Version	The current ADSL driver version loaded on your device
Bootloader (CFE) Version	The version of the bootloader
Wireless Driver Version	The current version of wireless driver being used by your device
Device Info For 3G	
Network	The name of your 3G network
Link	The status of your 3G connection
USB Vendor	The manufacturer of the inserted 3G USB modem
USB Model	The manufacturers model number of the inserted 3G USB modem
Signal Strength	The level of signal that your 3G USB modem is receiving from your 3G service provider
SIM Info	Indicates whether or not your SIM card is activated and ready for use
3G Backup	Indicates whether you have set the 3G USB modem to act as failover for your ADSL connection
3G Backup Interface	Indicates the WAN interface that is to be back up
Line Rate - Upstream	The upstream line rate in Kbps (e.g. 256 Kbps)
Line Rate - Downstream	The downstream line rate in Kbps (e.g. 1500 Kbps)
LAN IPv4 Address	The IP address to access the 3G15Wn on the LAN side
WAN IP Address	The IP address to access the 3G15Wn on the WAN side
Default Gateway	The default gateway that your 3G15Wn communicates with
Primary DNS Server	The primary DNS server IP address
Secondary DNS Server	The secondary DNS server IP address

3G Settings

3G Settings

3G Interface

On this screen you are able to select the 3G USB modem that you wish to use as your Internet connection. The field will auto fill with any compatible 3G USB modem

3G WAN Interface Configuration

Choose Add, or Remove to configure 3G WAN interfaces.

Model	Interface	Remove
Huawei_3G_modem	usb/(usb)	<input type="checkbox"/>

3G WAN Service

From the 3G WAN Service page you are able to setup your 3G connection with advanced settings. Simply press **Add** to manually configure advanced settings for your 3G connection. You can add as many different configurations as you like. If you would like to remove any configurations at any time, tick the **remove** box and press the **remove** button.

3G Service Setup

Choose Add, or Remove to configure a 3G service.

Interface	Description	Type	Vlan8021p	VlanMuxId	ConnId	Igmp	NAT	Firewall	Remove
ppp0	ppp_usb	PPF over TTY	N/A	N/A	N/A	Disabled	Enabled	Enabled	<input type="checkbox"/>

PIN Configuration

This screen allows for changes to the 3G SIM card PIN code protection settings.

NOTE: If you have entered the incorrect PIN 3 times, your SIM card will be locked for your security. Please call your 3G Provider for assistance.

3G Settings > PIN Configuration

PIN Code Protection

PIN Lock

PIN Code:

Confirm PIN Code:

PIN Code Change

Old PIN Code:

New PIN Code:

Confirm PIN Code:

PIN Code Protection

PIN code protection prevents the use of a SIM card by unauthorized persons. To use the 3G internet service with this router however, the PIN code protection must be disabled. If the SIM card inserted into the Router is locked with a PIN code, the web user interface will display the following screen after login.

PIN Lock Off

If you wish to connect to the Internet using a PIN locked SIM card, you must first turn PIN code protection Off. Select PIN lock Off, enter the PIN Code twice. Please keep in mind you only have 3 attempts before your SIM card is locked. The remaining attempts' number shows how many attempts left. Contact Telstra if you require assistance. You can select Remember PIN Code to ON so you don't need to input the PIN code every time when the router turns on. Afterwards, click Apply. The following dialog box should now appear.

PIN Code Change

If you wish to change your PIN code for greater security, enable the PIN Code protection. Go to the previous section and follow the procedure listed under PIN Lock On.

After locking the SIM card, select PIN Code Change and enter your Old and New PIN codes in the fields provided. Keep in mind you only have 3 attempts before your SIM card is locked. The remaining attempts' number shows how many attempts left. Contact Telstra if you require assistance. Afterwards, click Apply to activate the change.

3G Backup Config

On this page you are able to configure your 3G15Wn to use 3G as a backup to ADSL. Therefore if you have both connection options available, should your ADSL connection fail, for whatever reason, then your 3G will automatically kick in to ensure you remain connected to the Internet

3G Settings > 3G Backup Configuration

Use this page to enable/disable the 3G Backup feature.

Enable 3G Backup

Check Interval(sec.):
 Retry times:
 IP Address:

Select a preferred wan interface to be backuped.

Selected WAN Interface ▼

Option	Description
Enable 3G backup	Check this box to enable your 3G15Wn to work with 3G backup
Check Interval	The time in seconds that you 3G15Wn will check continuously for your ADSL Internet Connection.
Retry times	How many times the 3G15Wn will retry
IP address	The Public IP address that you would like to use for checking the ADSL Internet connection by Pinging
Selected WAN Interface	The WAN interface that you would like to backup with 3G

3G

Allows you to set your preferred network type. You can choose between 3G only, GPRS (2G) only, 3G preferred and GPRS (2G) preferred.

Set prefer network type

▼

Wireless

Wireless

Setup/Basic

The Wireless submenu provides access to Wireless Local Area Network (WLAN) configuration settings including:

- Wireless network name (SSID)
- Channel restrictions (based on country)
- Security
- Access point or bridging behaviour
- Station information

This screen allows you to configure basic features of the wireless LAN interface. You can enable or disable the wireless LAN interface, hide the network from active scans, set the wireless network name (also known as SSID) and restrict the channel set based on country requirements. The Wireless Guest Network function adds extra networking security when connecting to remote hosts.

Wireless -- Basic

This page allows you to configure basic features of the wireless LAN interface. You can enable or disable the wireless LAN interface, hide the network from active scans, set the wireless network name (also known as SSID) and restrict the channel set based on country requirements. Click "Apply/Save" to configure the basic wireless options.

Enable Wireless
 Hide Access Point
 Clients Isolation
 Disable WMM Advertise
 Enable Wireless Multicast Forwarding (WMF)

SSID:
 BSSID:
 Country:
 Max Clients:

Wireless - Guest/Virtual Access Points:

Enabled	SSID	Hidden	Isolate Clients	Disable WMM Advertise	Enable WMF	Max Clients	BSSID
<input type="checkbox"/>	<input type="text" value="wl0_Guest1"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="16"/>	N/A
<input type="checkbox"/>	<input type="text" value="wl0_Guest2"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="16"/>	N/A
<input type="checkbox"/>	<input type="text" value="wl0_Guest3"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="16"/>	N/A

Option	Description
Enable Wireless	A checkbox that enables (default) or disables the wireless LAN interface. When selected, the Web UI displays Hide Access point, SSID, BSSID and Country settings.
Hide Access Point	Select Hide Access Point to protect the access point from detection by wireless active scans. To check AP status in Windows XP, open Network Connections from the start Menu and select View Available Network Connections. If the access point is hidden, it will not be listed there. To connect a client to a hidden access point, the station must add the access point manually to its wireless configuration.
Clients Isolation	<ol style="list-style-type: none"> 1. Prevents clients PC from seeing one another in My Network Places or Network Neighborhood. 2. Prevents one wireless client communicating with another wireless client.
Disable WMM Advertise	Stops the router from 'advertising' its Wireless Multimedia (WMM) functionality, which provides basic quality of service for time-sensitive applications (e.g. VoIP, Video).
Enable WMF	Stops the router from 'advertising' its Wireless Multimedia (WMM) functionality, which provides basic quality of service for time-sensitive applications (e.g. VoIP, Video).
SSID [1-32 characters]	Sets the wireless network name. SSID stands for Service Set Identifier. All stations must be configured with the correct SSID to access the WLAN. If the SSID does not match, that user will not be granted access.
BSSID	The BSSID is a 48bit identity used to identify a particular BSS (Basic Service Set) within an area. In Infrastructure BSS networks, the BSSID is the MAC (Media Access Control) address of the AP (Access Point) and in Independent BSS or ad hoc networks, the BSSID is generated randomly.
Country	A drop-down menu that permits worldwide and specific national settings. Each country listed below enforces specific regulations limiting channel range: <ul style="list-style-type: none"> • Australia = 1-13
Wireless Guest Network	The Guest SSID (Virtual Access Point) can be enabled by selecting the Enable Wireless Guest Network checkbox. Rename the Wireless Guest Network as you wish. NOTE: Remote wireless hosts cannot scan Guest SSIDs.

Security

Security settings are used to prevent unauthorised connection to your network. This can be as basic as a neighbouring user who detects and is able to connect through your wireless network, right through to actual malicious interference or 'hacking'. Whatever the case, it is a good practice to be aware of and to use wireless network security to safeguard your data and your network.

Prior to considering the details of wireless security – provided later – the Quick Security Setup explains how to implement basic security on your 3G15Wn wireless network

Wireless -- Security

This page allows you to configure security features of the wireless LAN interface. You may setup configuration manually.

Manual Setup AP

You can set the network authentication method, selecting data encryption, specify whether a network key is required to authenticate to this wireless network and specify the encryption strength. Click "Apply/Save" when done.

Select SSID:

Network Authentication:

WEP Encryption:

Encryption Strength:

Current Network Key:

Network Key 1:

Network Key 2:

Network Key 3:

Network Key 4:

Enter 13 ASCII characters or 26 hexadecimal digits for 128-bit encryption keys.
Enter 5 ASCII characters or 10 hexadecimal digits for 64-bit encryption keys

Option	Description
Select SSID	Pre configured to the default of NetComm Wireless. Can be changed in the Wireless > Setup section
Network Authentication	Here, you can select the type of wireless security you desire
WEP Encryption	The option to enable or disable your wireless security encryption
Encryption Strength	The strength/length of your wireless security key. 64 bit is default
Current Network Key	The current network key that is active. You have the choice of setting up to 4 different wireless security keys
Network Key 1	The value of network key 1. Default value is a1b2c3d4e5
Network Key 2	The value of network key 2
Network Key 3	The value of network key 3
Network key 4	The value of network key 4

Configuration

The following screen appears when you select Configuration. This screen allows you to control the following advanced features of the Wireless Local Area Network (WLAN) interface:

- Select the channel which you wish to operate from
- Force the transmission rate to a particular speed
- Set the fragmentation threshold
- Set the RTS threshold
- Set the wake-up interval for clients in power-save mode
- Set the beacon interval for the access point
- Set Xpress mode
- Program short or long preambles

NetComm Gateway Series - ADSL2+/3G Wireless N300 4-Port Modem Router

Click Save/Apply to set the advanced wireless configuration

Wireless -- Advanced

This page allows you to configure advanced features of the wireless LAN interface. You can select a particular channel on which to operate, force the transmission rate to a particular speed, set the fragmentation threshold, set the RTS threshold, set the wakeup interval for clients in power-save mode, set the beacon interval for the access point, set XPress mode and set whether short or long preambles are used. Click "Apply/Save" to configure the advanced wireless options.

Band:	<input type="text" value="2.4GHz"/>	Current: 1
Channel:	<input type="text" value="Auto"/>	
Auto Channel Timer(min)	<input type="text" value="0"/>	
802.11n/EWC:	<input type="text" value="Auto"/>	
Bandwidth:	<input type="text" value="20MHz in 2.4G Band and 40MHz in 5G Band"/>	Current: 20MHz
Control Sideband:	<input type="text" value="Lower"/>	Current: None
802.11n Rate:	<input type="text" value="Auto"/>	
802.11n Protection:	<input type="text" value="Auto"/>	
Support 802.11n Client Only:	<input type="text" value="Off"/>	
54g™ Rate:	<input type="text" value="1 Mbps"/>	
Multicast Rate:	<input type="text" value="Auto"/>	
Basic Rate:	<input type="text" value="Default"/>	
Fragmentation Threshold:	<input type="text" value="2346"/>	
RTS Threshold:	<input type="text" value="2347"/>	
DTIM Interval:	<input type="text" value="1"/>	
Beacon Interval:	<input type="text" value="100"/>	
Global Max Clients:	<input type="text" value="16"/>	
XPress™ Technology:	<input type="text" value="Disabled"/>	
Transmit Power:	<input type="text" value="100%"/>	
WMM(Wi-Fi Multimedia):	<input type="text" value="Disabled"/>	
WMM No Acknowledgement:	<input type="text" value="Disabled"/>	
WMM APSD:	<input type="text" value="Enabled"/>	

Option	Description
Band	The new amendment allows IEEE 802.11g units to fall back to speeds of 11 Mbps, so IEEE 802.11b and IEEE 802.11g devices can coexist in the same network. The two standards apply to the 2.4 GHz frequency band. IEEE 802.11g creates data-rate parity at 2.4 GHz with the IEEE 802.11a standard, which has a 54 Mbps rate at 5 GHz. (IEEE 802.11a has other differences compared to IEEE 802.11b or g, such as offering more channels.)
Channel	Allows selection of a specific channel (1-14) or Auto mode.
Auto Channel Timer	The Auto Channel times the length it takes to scan in minutes.
802.11n/EWC	An equipment interoperability standard setting based on IEEE 802.11n Draft 2.0 and Enhanced Wireless Consortium (EWC)
Bandwidth	Drop-down menu specifies the following bandwidth: 20MHz in 2.4G Band and 40 MHz in 5G Band, 20MHz in both bands and 40MHz in both bands
Control Sideband	This is available for 40MHz. Drop-down menu allows selecting upper sideband or lower sideband
802.11n Rate	Drop-down menu specifies the following fixed rates. The maximum rate for bandwidth, 20MHz, is 130MHz and the maximum bandwidth, 40MHz, is 270MHz
802.11n Protection	Turn off for maximized throughput. Turn on for greater security
Support 802.11n Client Only	The option to provide wireless Internet access only to clients who are operating at 802.11n speeds
54g Rate	In Auto (default) mode, your Router uses the maximum data rate and lowers the data rate dependent on the signal strength. The appropriate setting is dependent on signal strength. Other rates are discrete values between 1 to 54 Mbps.
Multicast rate	Setting for multicast packet transmission rate. (1-54 Mbps)
Basic Rate	Sets basic transmission rate.
Fragment Threshold	A threshold (in bytes) determines whether packets will be fragmented and at what size. Packets that exceed the fragmentation threshold of an 802.11 WLAN will be split into smaller units suitable for the circuit size. Packets smaller than the specified fragmentation threshold value however are not fragmented. Values between 256 and 2346 can be entered but should remain at a default setting of 2346. Setting the Fragmentation Threshold too low may result in poor performance.
RTS Threshold	Request To Send (RTS) specifies the packet size that exceeds the specified RTS threshold, which then triggers the RTS/CTS mechanism. Smaller packets are sent without using RTS/CTS. The default setting of 2347 (max length) will disables the RTS Threshold.
DTIM Interval	Delivery Traffic Indication Message (DTIM) is also known as Beacon Rate. The entry range is a value between 1 and 65535. A DTIM is a countdown variable that informs clients of the next window for listening to broadcast and multicast messages. When the AP has buffered broadcast or multicast messages for associated clients, it sends the next DTIM with a DTIM Interval value. AP Clients hear the beacons and awaken to receive the broadcast and multicast messages. The default is 1.
Beacon Interval	The amount of time between beacon transmissions in is milliseconds. The default is 100 ms and the acceptable range is 1 – 65535. The beacon transmissions identify the presence of an access point. By default, network devices passively scan all RF channels listening for beacons coming from access points. Before a station enters power save mode, the station needs the beacon interval to know when to wake up to receive the beacon.
Global Max Clients	Here you have the option of setting the limit of the number of clients who can connect to your wireless network
Xpress Technology	Broadcom's Xpress™ Technology is compliant with draft specifications of two planned wireless industry standards. It has been designed to improve wireless network efficiency. Default is disabled
Transmit Power	The option of decreasing the transmitting power of your wireless signal
WMM	You can choose the enable or disable WMM which allows for priority of certain data over the wireless network
WMM No Acknowledgement	Refers to the acknowledge policy used at the MAC level. Enabling No Acknowledgement can result in more efficient throughput but higher error rates in a noisy Radio Frequency (RF) environment
WMM APSD	Automatic Power Save Delivery. Enable this to save power

MAC filter

This screen appears when Media Access Control (MAC) Filter is selected. This option allows access to be restricted based upon the unique 48-bit MAC address.

To add a MAC Address filter, click the **Add** button shown below.

To delete a filter, select it from the table below and click the **Remove** button.

Wireless -- MAC Filter

Select SSID:

MAC Restrict Mode: Disabled Allow Deny

Option	Description
MAC Restrict Mode	Disabled – Disables MAC filtering Allow: Permits access for the specified MAC addresses NOTE: Add a wireless device's MAC address before clicking the Allow radio button or else you will need to connect to the Router's web user interface using the supplied yellow Ethernet cable and add the wireless device's MAC address.
Deny	Rejects access for the specified MAC addresses
MAC Address	Lists the MAC addresses subject to the MAC Restrict Mode. The Add button prompts an entry field that requires you type in a MAC address in a two-character, 6-byte convention: xx:xx:xx:xx:xx:xx where xx are hexadecimal numbers. A maximum of 60 MAC addresses can be added.

Enter the MAC address on the screen below and click **Save/Apply**.

Wireless -- MAC Filter

Enter the MAC address and click "Apply/Save" to add the MAC address to the wireless MAC address filters.

MAC Address:

Wireless bridge

The following screen appears when selecting Wireless Bridge, and goes into a detailed explanation of how to configure wireless bridge features of the wireless LAN interface.

Click **Save/Apply** to implement new configuration settings.

Wireless -- Bridge

This page allows you to configure wireless bridge features of the wireless LAN interface. You can select Wireless Bridge (also known as Wireless Distribution System) to disable access point functionality. Selecting Access Point enables access point functionality. Wireless bridge functionality will still be available and wireless stations will be able to associate to the AP. Select Disabled in Bridge Restrict which disables wireless bridge restriction. Any wireless bridge will be granted access. Selecting Enabled or Enabled(Scan) enables wireless bridge restriction. Only those bridges selected in Remote Bridges will be granted access.

Click "Refresh" to update the remote bridges. Wait for few seconds to update.
Click "Apply/Save" to configure the wireless bridge options.

AP Mode:

Bridge Restrict:

Option	Description
AP Mode	Selecting Wireless Bridge (Wireless Distribution System) disables Access Point (AP) functionality while selecting Access Point enables AP functionality. In Access Point mode, wireless bridge functionality will still be available and wireless stations will be able to associate to the AP.
Bridge Restrict	Selecting Disabled in Bridge Restrict disables Wireless Bridge restriction, which means that any wireless bridge will be granted access. Selecting Enabled or Enabled (Scan) allows wireless bridge restriction. Only those bridges selected in Remote Bridges will be granted access. Click Refresh to update the station list when Bridge Restrict is enabled.

Station info

The following screen appears when you select Station Info, and shows authenticated wireless stations and their status.

Click the **Refresh** button to update the list of stations in the WLAN.

Wireless -- Authenticated Stations

This page shows authenticated wireless stations and their status.

MAC	Associated	Authorized	SSID	Interface
00:60:64:25:E6:AF	Yes		NetComm Wireless	wl0

Option	Description
MAC	The MAC address of any connected client
Associated	Lists all the stations that are associated with the Access Point, along with the amount of time since packets were transferred to and from each station. If a station is idle for too long, it is removed from this list.
Authorized	Lists those devices with authorized access.
SSID	The SSID of your wireless network
Interface	The wireless interface being used to connect

Management

Management

Device Settings

The Device Settings screens allow you to backup, retrieve and restore the default settings of your Router. It also provides a function for you to update your Routers firmware.

Backup

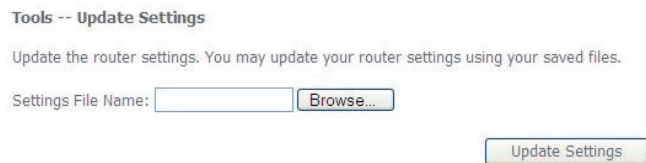
The following screen appears when Backup is selected. Click the **Backup Settings** button to save the current configuration settings.

You will be prompted to define the location of a backup file to save to your PC.



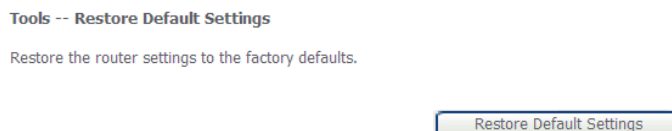
Update

The following screen appears when selecting Update from the submenu. By clicking on the **Browse** button, you can locate a previously saved filename as the configuration backup file. Click on the **Update settings** to load it



Restore Default

The following screen appears when selecting Restore Default. By clicking on the **Restore Default Settings** button, you can restore your Routers default firmware settings. To restore system settings, reboot your Router.



NOTE: The default settings can be found in the section Default Settings.

Once you have selected the Restore Default Settings button, the following screen will appear. Close the window and wait 2 minutes before reopening your browser. If required, reconfigure your PCs IP address to match your new configuration (see section 3.2 TCP/IP Settings for details).

After a successful reboot, the browser will return to the Device Info screen. If the browser does not refresh to the default screen, close and restart the browser.

NOTE: The Restore Default function has the same effect as the reset button. The device board hardware and the boot loader support the reset to default button. If the reset button is continuously pushed for more than 5 seconds (and not more than 12 seconds), the boot loader will erase the configuration settings saved on flash memory.

Update Firmware

The following screen appears when selecting Update Firmware. By following this screens steps, you can update your Routers firmware. Manual device upgrades from a locally stored file can also be performed using the following screen.

Management > Device Settings > Update Firmware

Step 1: Obtain the latest Firmware file from NetComm.

Step 2: Enter the path to the file location in the box below or click the "Browse" button to locate the file.

Step 3: Click the "Update Software" button once to upload the new Firmware file.

NOTE: The update process for the Gateway takes about 2 minutes to complete, and for the 3G modem takes about 10 minutes, and your Gateway will reboot. Please DO NOT close the Browser and reload/or change the webpage during the update process.

Software File Name:

- 1: Obtain an updated software image file
- 2: Enter the path and filename of the firmware image file in the Software File Name field or click the **Browse** button to locate the image file.
- 3: Click the **Update Software** button once to upload and install the file.

NOTE: The update process will take about 2 minutes to complete. The Router will reboot and the browser window will refresh to the default screen upon successful installation. It is recommended that you compare the Software Version at the top of the Basic screen (WUI homepage) with the firmware version installed, to confirm the installation was successful.

SNMP

The Simple Network Management Protocol (SNMP) allows a network administrator to monitor a network by retrieving settings on remote network devices. To do this, the administrator typically runs an SNMP management station program such as MIB browser on a local host to obtain information from the SNMP agent, in this case the 3G15Wn (if SNMP enabled). An SNMP 'community' performs the function of authenticating SNMP traffic. A 'community name' acts as a password that is typically shared among SNMP agents and managers.

SNMP - Configuration

Simple Network Management Protocol (SNMP) allows a management application to retrieve statistics and status from the SNMP agent in this device.

Select the desired values and click "Apply" to configure the SNMP options.

SNMP Agent Disable Enable

Read Community:

Set Community:

System Name:

System Location:

System Contact:

Trap Manager IP:

Option	Description
Read Community	Read device settings
Set Community	Read and change device settings
System Name	Default = 3G15Wn
System Location	User defined value
System Contact	User defined value
Trap Manager IP	IP address of admin machine

TR-069 client

WAN Management Protocol (TR-069) allows an Auto-Configuration Server (ACS) to perform auto-configuration, provision, collection, and diagnostics to this device.

TR-069 client - Configuration

WAN Management Protocol (TR-069) allows a Auto-Configuration Server (ACS) to perform auto-configuration, provision, collection, and diagnostics to this device.

Select the desired values and click "Apply/Save" to configure the TR-069 client options.

Inform Disable Enable

Inform Interval:

ACS URL:

ACS User Name:

ACS Password:

WAN Interface used by TR-069 client:

Display SOAP messages on serial console Disable Enable

Connection Request Authentication

Connection Request User Name:

Connection Request Password:

Connection Request URL:

Option	Description
Inform	Disable/Enable TR-069 client on the CPE
Inform Interval	The duration in seconds of the interval for which the CPE MUST attempt to connect with the ACS and call the Inform method
ACS URL	URL for the CPE to connect to the ACS using the CPE WAN Management Protocol. This parameter MUST be in the form of a valid HTTP or HTTPS URL. An HTTPS URL indicates that the ACS supports SSL. The "host" portion of this URL is used by the CPE for validating the certificate from the ACS when using certificate-based authentication
ACS User Name	Username used to authenticate the CPE when making a connection to the ACS using the CPE WAN Management Protocol. This username is used only for HTTP-based authentication of the CPE.
ACS Password	Password used to authenticate the CPE when making a connection to the ACS using the CPE WAN Management Protocol. This password is used only for HTTP-based authentication of the CPE
WAN Interface used by TR-069 client	Choose which WAN interface that TR-069 would use for communication with TR-069 Server.
Connection Request Authentication	Enable/Disable authentication of ACS making a Connection Request to the CPE.
Connection Request User Name	Username used to authenticate an ACS making a connection request to the CPE
Connection Request Password	Password used to authenticate an ACS making a connection request to the CPE
Connection Request URL	URL used to authenticate an ACS making a connection request to the CPE

SNTP

This screen allows you to configure the time settings of your Router.

Time settings

This page allows you to the modem's time configuration.

Automatically synchronize with Internet time servers

First NTP time server:	Other	0.netcomm.pool.ntp.org
Second NTP time server:	Other	1.netcomm.pool.ntp.org
Third NTP time server:	None	
Fourth NTP time server:	None	
Fifth NTP time server:	None	
Time zone offset:	(GMT+10:00) Canberra, Melbourne, Sydney	

Apply/Save

Option	Description
First NTP timeserver:	Select the required server.
Second NTP timeserver:	Select second timeserver, if required.
Time zone offset:	Select the local time zone.

NOTE: SNTP must be activated to use Parental Control

Access Control

The Access Control option found in the Management drop down menu, configures access related parameters in the following three areas:

- Services
- Passwords
- Save/Reboot

Access Control is used to control local and remote management settings for your Router.

Services

The Service Control List (SCL) allows you to enable or disable your Local Area Network (LAN) or Wireless Area Network (WAN) services by ticking the checkbox as illustrated below. These access services are available: FTP, HTTP, ICMP, SNMP, SSH, TELNET, and TFTP. Click Save/Apply to continue.

Management > Access Control > Services

A Service Control List ("SCL") enables or disables services from being used.

The following ports are not recommended for HTTP remote management in case conflict with them for other management purpose in some particular case (21, 2121, 22, 2222, 23, 2323, 69, 6969, 161, 16116)

Services	WAN
FTP	<input type="checkbox"/> Enable
HTTP	<input type="checkbox"/> Enable <input type="text" value="80"/> port
ICMP	<input type="checkbox"/> Enable
SNMP	<input type="checkbox"/> Enable
SSH	<input type="checkbox"/> Enable
TELNET	<input type="checkbox"/> Enable
TFTP	<input type="checkbox"/> Enable

Save/Apply

Passwords

The Passwords option configures your account access password for your Router. Access to the device is limited to the following three user accounts:

- admin is to be used for local unrestricted access control
- support is to be used for remote maintenance of the device
- user is to be used to view information and update device firmware

Use the fields illustrated in the screen below to change or create your password. Passwords must be 16 characters or less with no spaces. Click Save/Apply to continue.

Access Control -- Passwords

Access to your router is controlled through three user accounts: admin, support, and user.

The user name "admin" has unrestricted access to change and view configuration of your router.

The user name "support" is used to allow an ISP technician to access your router for maintenance and to run diagnostics.

The user name "user" can access the router, view configuration settings and statistics, as well as, update the router's software.

Use the fields below to enter up to 16 characters and click "Apply/Save" to change or create passwords. Note: Password cannot contain a space.

Username:

Old Password:

New Password:

Confirm Password:

Save/Reboot

This function saves the current configuration settings and reboots your Router.

Click the button below to reboot the router.

NOTE 1: It may be necessary to reconfigure your TCP/IP settings to adjust for the new configuration. For example, if you disable the Dynamic Host Configuration Protocol (DHCP) server you will need to apply Static IP settings.

NOTE 2: If you lose all access to your web user interface, simply press the reset button on the rear panel for 5-7 seconds to restore default settings

Advanced

Advanced

ATM interface

This page allows you to set your DSL connection with advanced configuration options. Select **Add** to include a new configuration and select **Remove** to delete the selected configuration. You can add as many configurations as you like

DSL ATM Interface Configuration

Choose Add, or Remove to configure DSL ATM interfaces.

Interface	Vpi	Vci	DSL Latency	Category	Link Type	Connection Mode	QoS	Remove
atm0	8	35	Path0	UBR	EoA	DefaultMode	Enabled	<input type="checkbox"/>

[Add](#) [Remove](#)

Option	Description
Interface	Shows the Interface Name
Vpi	Shows the value of Vpi
Vci	Shows the value of Vci
DSL Latency	The value of the DSL latency
Category	Shows the ATM service classes
Link Type	Shows the type of the Link
Connection Mode	Shows the selected mode of connection
QoS	Shows the status of the QoS function
Remove	Select to remove ATM interface configuration

WAN service

Select WAN from the Device Info menu to display the status of all configured PVC(s).

Wide Area Network (WAN) Service Setup

Choose Add, Remove or Edit to configure a WAN service over a selected interface.

ETH and PTM/ATM service can not coexist.

Interface	Description	Type	Vlan8021p	VlanMuxId	ConnId	Igmp	NAT	Firewall	Remove	Edit
-----------	-------------	------	-----------	-----------	--------	------	-----	----------	--------	------

[Add](#) [Remove](#)

LAN

This screen allows you to configure the Local Area Network (LAN) interface on your Router.

Local Area Network (LAN) Setup

Configure the Router IP Address and Subnet Mask for LAN interface. GroupName Default

IP Address:

Subnet Mask:

Enable IGMP Snooping

Enable LAN side firewall

Disable DHCP Server

Enable DHCP Server

Start IP Address:

End IP Address:

Leased Time (hour):

Static IP Lease List: (A maximum 32 entries can be configured)

MAC Address	IP Address	Remove
<input type="text"/>	<input type="text"/>	<input type="button" value="Remove"/>

Configure the second IP Address and Subnet Mask for LAN interface

See the field descriptions below for more details.

Option	Description
IP Address	Enter the IP address for the LAN interface
Subnet Mask	Enter the subnet mask for the LAN interface
Enable IGMP Snooping	Enable by ticking the box Standard Mode: In standard mode, multicast traffic will flood to all bridge ports when no client subscribes to a multicast group. Blocking Mode: In blocking mode, the multicast data traffic will be blocked. When there are no client subscriptions to a multicast group, it will not flood to the bridge ports.
Enable LAN side Firewall	Check box to enable Firewall on LAN
Disable DHCP Server	Disables the DHCP server. Only to be done if Static IP address is set up
Enable DHCP Server	Select Enable DHCP server and enter your starting and ending IP addresses and the lease time. This setting configures the router to automatically assign IP, default gateway and DNS server addresses to every DHCP client on your LAN
Enable DHCP Server Relay	To relay DHCP requests from the subnet with no DHCP server on it to a DHCP server on other subnets. DHCP Server Relay is disabled by default. To access enable DHCP relay, please un-tick NAT enable first, that means to disable NAT first, and then press save button.
Configure the second IP Address and Subnet Mask for LAN Interface	Configure a second IP address by ticking the checkbox shown below and enter the following information: Enter the secondary IP address for the LAN interface. Enter the secondary subnet mask for the LAN interface.

NAT

Port Forwarding

Port Forwarding allows you to direct incoming traffic from the Internet side (identified by Protocol and External port) to the internal server with a private IP address on the LAN side. The Internal port is required only if the external port needs to be converted to a different port number used by the server on the LAN side. A maximum of 32 entries can be configured.

NAT -- Virtual Servers Setup

Virtual Server allows you to direct incoming traffic from WAN side (identified by Protocol and External port) to the internal server with private IP address on the LAN side. The Internal port is required only if the external port needs to be converted to a different port number used by the server on the LAN side. A maximum 32 entries can be configured.

Server Name	External Port Start	External Port End	Protocol	Internal Port Start	Internal Port End	Server IP Address	WAN Interface	Remove
-------------	---------------------	-------------------	----------	---------------------	-------------------	-------------------	---------------	--------

To add a Virtual Server, click the **Add** button. The following screen will display.

NAT -- Virtual Servers

Select the service name, and enter the server IP address and click "Apply/Save" to forward IP packets for this service to the specified server. NOTE: The "Internal Port End" cannot be modified directly. Normally, it is set to the same value as "External Port End". However, if you modify "Internal Port Start", then "Internal Port End" will be set to the same value as "Internal Port Start".

Remaining number of entries that can be configured:32

Use Interface:

Service Name:

Select a Service:

Custom Service:

Server IP Address:

External Port Start	External Port End	Protocol	Internal Port Start	Internal Port End
		TCP		
		TCP		
		TCP		
		TCP		
		TCP		
		TCP		
		TCP		
		TCP		
		TCP		
		TCP		
		TCP		
		TCP		
		TCP		
		TCP		
		TCP		
		TCP		
		TCP		
		TCP		

Option	Description
Select a Service Or Custom Server	User should select the service from the list. Or Create a customer server and enter a name for the server
Server IP Address	Enter the IP address for the server.
External Port Start	Enter the starting external port number (when you select Custom Server). When a service is selected the port ranges are automatically configured.
External Port End	Enter the ending external port number (when you select Custom Server). When a service is selected the port ranges are automatically configured.
Protocol	User can select from: TCP, TCP/UDP or UDP.
Internal Port Start	Enter the internal port starting number (when you select Custom Server). When a service is selected the port ranges are automatically configured
Internal Port End	Enter the internal port ending number (when you select Custom Server). When a service is selected the port ranges are automatically configured.

Port Triggering

Some applications require specific ports in the Router's firewall to be open for access by remote parties. Port Triggering opens up the 'Open Ports' in the firewall when an application on the LAN initiates a TCP/UDP connection to a remote party using the 'Triggering Ports'. The Router allows the remote party from the WAN side to establish new connections back to the application on the LAN side using the 'Open Ports'. A maximum 32 entries can be configured.

NAT -- Port Triggering Setup

Some applications require that specific ports in the Gateway's firewall be opened for access by the remote parties. Port Trigger dynamically opens up the 'Open Ports' in the firewall when an application on the LAN initiates a TCP/UDP connection to a remote party using the 'Triggering Ports'. The Gateway allows the remote party from the WAN side to establish new connections back to the application on the LAN side using the 'Open Ports'. A maximum 32 entries can be configured.

Application Name	Trigger		Open		WAN Interface	Remove
	Protocol	Port Range Start End	Protocol	Port Range Start End		

To add a Trigger Port, simply click the **Add** button. The following will be displayed.

NAT -- Port Triggering

Some applications such as games, video conferencing, remote access applications and others require that specific ports in the Router's firewall be opened for access by the applications. You can configure the port settings from this screen by selecting an existing application or creating your own (Custom application) and click "Save/Apply" to add it.
 Remaining number of entries that can be configured: 32

Use Interface:

Application Name:

Select an application:

Custom application:

Trigger Port Start	Trigger Port End	Trigger Protocol	Open Port Start	Open Port End	Open Protocol
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	TCP
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	TCP
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	TCP
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	TCP
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	TCP
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	TCP
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	TCP
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	TCP
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	TCP

Option	Description
Select an Application or Custom Application	User should select the application from the list. Or User can enter the name of their choice.
Trigger Port Start	Enter the starting trigger port number (when you select custom application). When an application is selected, the port ranges are automatically configured.
Trigger Port End	Enter the ending trigger port number (when you select custom application). When an application is selected, the port ranges are automatically configured.
Trigger Protocol	TCP, TCP/UDP or UDP.
Open Port Start	Enter the starting open port number (when you select custom application). When an application is selected, the port ranges are automatically configured.
Open Port End	Enter the ending open port number (when you select custom application). When an application is selected, the port ranges are automatically configured.
Open Protocol	TCP, TCP/UDP or UDP

DMZ Host

Your Router will forward IP packets from the Wireless Area Network (WAN) that do not belong to any of the applications configured in the Virtual Servers table to the DMZ host computer.

Enter the computer's IP address and click Apply to activate the DMZ host. Clear the IP address field and click **Apply** to deactivate the DMZ host.

NAT -- DMZ Host

The router will forward IP packets from the WAN that do not belong to any of the applications configured in the Virtual Servers table to the DMZ host computer.

Enter the computer's IP address and click "Apply" to activate the DMZ host.

Clear the IP address field and click "Apply" to deactivate the DMZ host.

DMZ Host IP Address:

Security

Your Router can be secured with IP Filtering or Parental Control functions.

IP Filtering

The IP Filtering screen sets filter rules that limit incoming and outgoing IP traffic. Multiple filter rules can be set with at least one limiting condition. All conditions must be fulfilled when individual IP packets pass filter.

Outgoing IP Filter

The default setting for Outgoing traffic is ACCEPTED. Under this condition, all outgoing IP packets that match the filter rules will be BLOCKED.

Outgoing IP Filtering Setup

By default, all outgoing IP traffic from LAN is allowed, but some IP traffic can be **BLOCKED** by setting up filters.

Choose Add or Remove to configure outgoing IP filters.

Filter Name	Protocol	Source Address / Mask	Source Port	Dest. Address / Mask	Dest. Port	Remove
<input type="button" value="Add"/> <input type="button" value="Remove"/>						

To add a filtering rule, click the **Add** button. The following screen will display.

Add IP Filter -- Outgoing

The screen allows you to create a filter rule to identify outgoing IP traffic by specifying a new filter name and at least one condition below. All of the specified conditions in this filter rule must be satisfied for the rule to take effect. Click 'Apply/Save' to save and activate the filter.

Filter Name:

Protocol:

Source IP address:

Source Subnet Mask:

Source Port (port or port:port):

Destination IP address:

Destination Subnet Mask:

Destination Port (port or port:port):

Filter Name	The filter rule label
Protocol	TCP, TCP/UDP, UDP or ICMP
Source IP address	Enter source IP address Source Subnet Mask
Destination IP address	Enter source subnet mask
Source Port (port or port:port)	Enter source port number or port range
Destination IP address	Enter destination IP address
Destination Subnet Mask	Enter destination subnet mask
Destination port (port or port:port)	Enter destination port number or range

Click **Save/Apply** to save and activate the filter.

Incoming IP Filter

The default setting for all Incoming traffic is BLOCKED. Under this condition only those incoming IP packets that match the filter rules will be ACCEPTED.

Incoming IP Filtering Setup

When the firewall is enabled on a WAN or LAN interface, all incoming IP traffic is BLOCKED. However, some IP traffic can be **ACCEPTED** by setting up filters.

Choose Add or Remove to configure incoming IP filters.

Filter Name	Interfaces	Protocol	Source Address / Mask	Source Port	Dest. Address / Mask	Dest. Port	Remove
<input type="button" value="Add"/> <input type="button" value="Remove"/>							

To add a filtering rule, click the **Add** button. The following screen will display.

Add IP Filter -- Incoming

The screen allows you to create a filter rule to identify incoming IP traffic by specifying a new filter name and at least one condition below. All of the specified conditions in this filter rule must be satisfied for the rule to take effect. Click 'Apply/Save' to save and activate the filter.

Filter Name:

Protocol:

Source IP address:

Source Subnet Mask:

Source Port (port or port:port):

Destination IP address:

Destination Subnet Mask:

Destination Port (port or port:port):

WAN Interfaces (Configured in Routing mode and with firewall enabled) and LAN Interfaces
 Select one or more WAN/LAN interfaces displayed below to apply this rule.

- Select All
 ppp_usb/ppp1
 pppoe_0_8_35/ppp0
 br0/br0

Please refer to the Outgoing IP Filter table for field descriptions.

Click **Save/Apply** to save and activate the filter.

Parental Control

The Parental Control feature allows you to take advanced measures to ensure the computers connected to the LAN are used only when and how prescribed

Time Restriction

This Parental Control allows you to restrict access from a Local Area Network (LAN) to an outside network through the Router on selected days at certain times. Make sure to activate the Internet Time server synchronization as described in the SNTP section of this manual, so that the scheduled times match your local time.

Access Time Restriction -- A maximum 16 entries can be configured.

Username	MAC	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start	Stop	Remove
<input type="button" value="Add"/> <input type="button" value="Remove"/>											

Click **Add** to display the following screen.

Access Time Restriction

This page adds time of day restriction to a special LAN device connected to the Router. The 'Browser's MAC Address' automatically displays the MAC address of the LAN device where the browser is running. To restrict other LAN device, click the "Other MAC Address" button and enter the MAC address of the other LAN device. To find out the MAC address of a Windows based PC, go to command window and type "ipconfig /all".

User Name:

Browser's MAC Address:

Other MAC Address:

Days of the week: Mon Tue Wed Thu Fri Sat Sun

Start Blocking Time (hh:mm):

End Blocking Time (hh:mm):

See instructions below and click **Save/Apply** to apply the settings.

Option	Description
User Name:	A user-defined label for this restriction
Browser's MAC Address	MAC address of the PC running the browser
Other MAC Address:	MAC address of another LAN device
Days of the week	The days the restrictions apply
Start Blocking Time	The time the restrictions start
End Blocking Time	The time the restrictions end

URL filter

With the URL filter, you are able to add certain websites or URLs to a safe or blocked list. This will provide you added security to ensure any website you deem unsuitable will not be able to be seen by anyone who is accessing the Internet via the 3G15Wn.

Simply check Exclude or Include and then click **Add** to enter the URL you wish added to a list

URL Filter -- Please select the list type first then configure the list entries. Maximum 100 entries can be configured.

URL List Type: Exclude Include

Address	Port	Remove
<input type="button" value="Add"/> <input type="button" value="Remove"/>		

Once you have chosen to add a URL to the list you will be prompted to enter the address. Simply type it in and select **Apply/Save**

Parental Control -- URL Filter Add

Enter the URL address and port number then click "Apply/Save" to add the entry to the URL filter.

URL Address:

Port Number: (Default 80 will be applied if leave blank.)

Quality of Service

Quality of Service offers a defined level of performance in a data communications system - for example the ability to guarantee that video traffic is given priority over other network traffic to ensure that video streaming is not disrupted by other network requirements. This means that should you be streaming video and someone else in the house starts downloading a big file, the download won't disrupt the flow of video data.

QoS -- Queue Management Configuration

If Enable QoS checkbox is selected, choose a default DSCP mark to automatically mark incoming traffic without reference to a particular classifier. Click 'Apply/Save' button to save it.

Note: If Enable QoS checkbox is not selected, all QoS will be disabled for all interfaces.

Note: The default DSCP mark is used to mark all egress packets that do not match any classification rules.

Enable QoS

Apply/Save

Queue configuration

This function follows the Differentiated Services rule of IP QoS. You can create a new Queue rule by assigning an Interface, Enable/Disable and Precedence. The router uses various queuing strategies to tailor performance to user requirements

QoS Queue Setup -- A maximum 16 entries can be configured.

If you disable WMM function in Wireless Page, queues related to wireless will not take effects

The QoS function has been disabled. Queues would not take effects.

Name	Key	Interface	Precedence	DSL Latency	PTM Priority	Enable	Remove
WMM Voice Priority	1	wl0	1			Enabled	
WMM Voice Priority	2	wl0	2			Enabled	
WMM Video Priority	3	wl0	3			Enabled	
WMM Video Priority	4	wl0	4			Enabled	
WMM Best Effort	5	wl0	5			Enabled	
WMM Background	6	wl0	6			Enabled	
WMM Background	7	wl0	7			Enabled	
WMM Best Effort	8	wl0	8			Enabled	

Add Enable Remove

Click **Add** to display the following screen

QoS Queue Configuration

The screen allows you to configure a QoS queue entry and assign it to a specific network interface. Each of the queues can be configured for a specific precedence. The queue entry configured here will be used by the classifier to place ingress packets appropriately. **Note: Lower integer values for precedence imply higher priority for this queue relative to others** Click 'Apply/Save' to save and activate the queue.

Name:

Enable:

Interface:

Precedence:

Apply/Save

QoS classification

QoS Classification Setup -- A maximum 32 entries can be configured.

Choose Add or Remove to configure network traffic classes.

If you disable WMM function in Wireless Page, classification related to wireless will not take effects

The QoS function has been disabled. Classification rules would not take effects.

CLASSIFICATION CRITERIA														CLASSIFICATION RESULTS					
Class Name	Order	Class Intf	Ether Type	SrcMAC/ Mask	DstMAC/ Mask	SrcIP/ Mask	DstIP/ Mask	Proto	Src Port	Dst Port	DSCP Check	802.1P Check	Queue Key	DSCP Mark	802.1P Mark	VlanID Tag	Rate Control (kbps)	Enable	Remove

Click **Add** to configure network traffic classes.

Add Network Traffic Class Rule

The screen creates a traffic class rule to classify the upstream traffic, assign queue which defines the precedence and the interface and optionally overwrite the IP header DSCP byte. A rule consists of a class name and at least one condition below. All of the specified conditions in this classification rule must be satisfied for the rule to take effect. Click 'Save/Apply' to save and activate the rule.

Traffic Class Name:

Rule Order:

Rule Status:

Specify Classification Criteria
A blank criterion indicates it is not used for classification.

Class Interface:

Ether Type:

Source MAC Address:

Source MAC Mask:

Destination MAC Address:

Destination MAC Mask:

Specify Classification Results
Must select a classification queue. A blank mark or tag value means no change.

Assign Classification Queue:

Mark Differentiated Service Code Point (DSCP):

Mark 802.1p priority:

Tag VLAN ID [0-4094]:

Set Rate Control(kbps):

This screen creates a traffic class rule to classify the upstream traffic, assign queuing priority and optionally overwrite the IP header TOS byte. A rule consists of a class name and at least one condition below. All of the specified conditions in this classification rule must be satisfied for the rule to take effect.

Click **Save/Apply** to save and activate the rule.

Routing

Default Gateway, Static Route, Policy Routing and Dynamic Route settings can be found in the Routing link as illustrated below.

Default gateway

Select your preferred WAN interface from the drop down box.

Routing -- Default Gateway

Select a preferred wan interface as the system default gateway.

Selected WAN Interface

Static route

The Static Route screen displays the configured static routes.

Click the **Add** or **Remove** buttons to change settings.

Routing -- Static Route (A maximum 32 entries can be configured)

Destination	Subnet Mask	Gateway	Interface	Remove
				<input type="button" value="Add"/> <input type="button" value="Remove"/>

Click the **Add** button to display the following screen.

Routing -- Static Route Add

Enter the destination network address, subnet mask, gateway AND/OR available WAN interface then click "Apply/Save" to add the entry to the routing table.

Destination Network Address:

Subnet Mask:

Use Interface

Use Gateway IP Address

Enter Destination Network Address, Subnet Mask, Gateway IP Address and/or WAN Interface. Then click **Save/Apply** to add the entry to the routing table.

Policy routing

Allows you to add policy rules to certain situations

Policy Routing Setting -- A maximum 8 entries can be configured.

Policy Name	Source IP	LAN Port	WAN	Default GW	Remove
-------------	-----------	----------	-----	------------	--------

Click **Add** to display the following screen

Policy Routing Setup
Enter the policy name, policies, and WAN interface then click "Save/Apply" to add the entry to the policy routing table.
Note: If selected "MER" as WAN interface, default gateway must be configured.

Policy Name:

Physical LAN Port:

Source IP:

Use Interface:

Default Gateway:

Dynamic router

To activate this option, select the Enabled radio button for Global RIP Mode.

To configure an individual interface, select the desired RIP version and operation, followed by placing a check in the Enabled checkbox for that interface. Click **Save/Apply** to save the configuration and to start or stop dynamic routing.

Routing -- RIP Configuration

NOTE: RIP CANNOT BE CONFIGURED on the WAN interface which is PPP mode. And the WAN interface which has NAT enabled only can be configured the operation mode as passive.

To activate RIP for the WAN Interface, select the desired RIP version and operation and place a check in the 'Enabled' checkbox. To stop RIP on the WAN Interface, uncheck the 'Enabled' checkbox. Click the 'Apply/Save' button to star/stop RIP and save the configuration.

Interface	Version	Operation	Enabled
-----------	---------	-----------	---------

WAN Interface not exist for RIP.

DNS

DNS server

This page allows user to enable automatic DNS from the ISP or specify their own DNS server address manually

DNS Server Configuration

Select the configured WAN interface for DNS server information OR enter the static DNS server IP Addresses for single PVC with IPoA, static IPoE protocol.

Obtain DNS info from a WAN interface:
WAN Interface selected:

Use the following Static DNS IP address:
Primary DNS server:
Secondary DNS server:

Dynamic DNS

The Dynamic DNS service allows a dynamic IP address to be aliased to a static hostname in any of a selection of domains, allowing the router to be more easily accessed from various locations on the internet.

Dynamic DNS

The Dynamic DNS service allows you to alias a dynamic IP address to a static hostname in any of the many domains, allowing your Gateway to be more easily accessed from various locations on the Internet.

Choose Add or Remove to configure Dynamic DNS.

Hostname	Username	Service	Interface	Remove
<input type="button" value="Add"/> <input type="button" value="Remove"/>				

Note: The Add/Remove buttons will be displayed only if the router has been assigned an IP address from the remote server.

To add a dynamic DNS service, click the **Add** button and this screen will display.

Add Dynamic DNS

This page allows you to add a Dynamic DNS address from DynDNS.org or TZO.

D-DNS provider:

Hostname:

Interface:

DynDNS Settings

Username:

Password:

Name	Description
D-DNS provider	Select a dynamic DNS provider from the list
Hostname	Enter the name for the dynamic DNS server
Interface	Select the interface from the list
Username	Enter the username for the dynamic DNS server
Password	Enter the password for the dynamic DNS server

DSL

This page allows the user to modify the DSL modulation settings on the unit. By changing the settings, the user can specify which DSL modulation that the modem will use.

DSL Settings

Select the modulation below.

G.Dmt Enabled
 G.lite Enabled
 T1.413 Enabled
 ADSL2 Enabled
 AnnexL Enabled
 ADSL2+ Enabled
 AnnexM Enabled

Select the phone line pair below.

Inner pair
 Outer pair

Capability

Bitswap Enable
 SRA Enable

UPnP

Simply check or uncheck the box and press **Apply/Save** to enable or disable the UPnP protocol

Upnp Configuration

Enable or disable Upnp protocol.

DNS proxy

To enable DNS Proxy, tick the corresponding checkbox and then enter host and Domain name, as the example shown below. Click **Apply/Save** to continue.

Dns Proxy Configuration

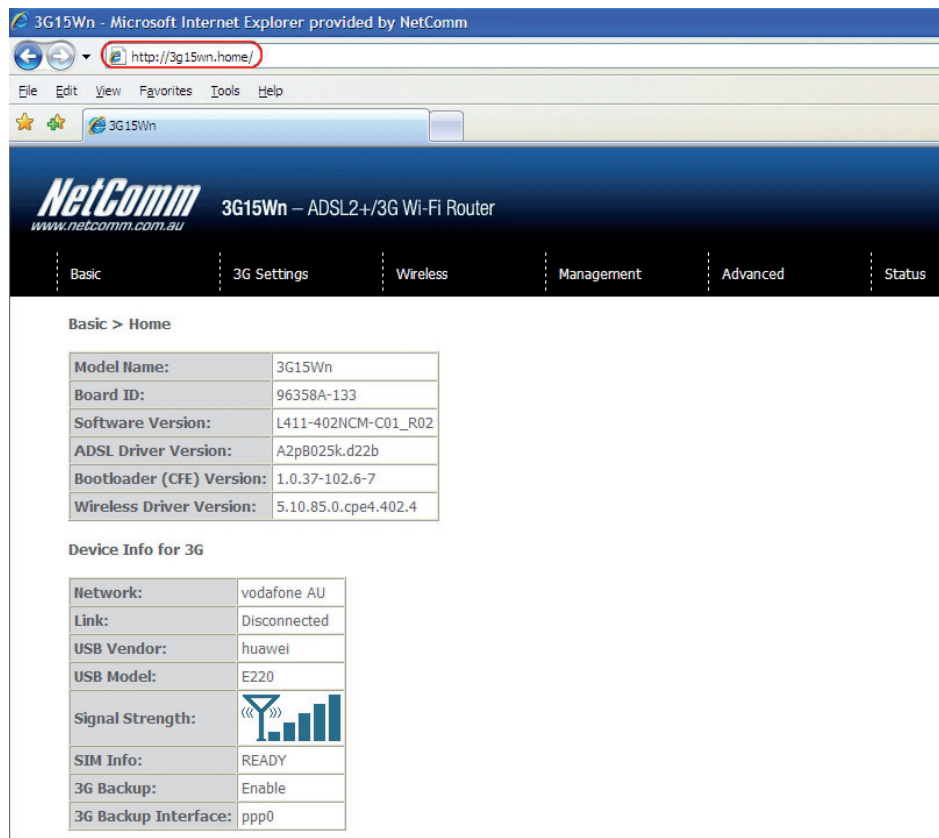
Enable or disable Dns proxy.

Host name of the modem:

Domain name of the LAN network:

The Host Name and Domain name are combined to form a unique label that is mapped to the router IP address. This can be used to access the WebUI with a local name rather than by using the router IP address.

The figure below shows an example of this which is the default setting.



USB Storage

This page allows you to enable/disable the USB port of the 3G15Wn to be used as a mass storage server

Please see Appendix B for more details on setting up your router to work with Storage Server functionality

Note: These settings are for advanced users. We recommend that you do not change it if you are unsure of what you are doing. If you do run into problems, you can reset the Gateway back to default settings. To do this, insert a pointed object (like a straightened paperclip) into the hole at the back of the Gateway labelled 'Reset'. Press and hold the reset button till the power light starts flashing - then release the button, you will need to run the Install CD that came in your kit again once you reset the Gateway

Advanced > USB Storage settings

USB Status: **detected**

This page allows you to enable / disable USB storage .

Enable USB storage

Netbios Name:

Directory Name:

Save/Apply

Print Server

This page allows you to enable/disable the USB port of the 3G15Wn to be used as a print server

Please see Appendix A for more details on setting up your router to work with Print Server functionality

Print Server settings

This page allows you to enable / disable printer support.

Enable on-board print server.

Apply/Save

Interface grouping

Interface grouping supports multiple ports to PVC and bridge groups. Each group performs as an independent network. To use this feature, you must create mapping groups with appropriate LAN and WAN interfaces using the Add button.

The Remove button removes mapping groups, returning the ungrouped interfaces to the default group. Only the default group has an IP interface.

Interface Grouping -- A maximum 16 entries can be configured

Interface Grouping supports multiple ports to PVC and bridging groups. Each group will perform as an independent network. To support this feature, you must create mapping groups with appropriate LAN and WAN interfaces using the Add button. The Remove button will remove the grouping and add the ungrouped interfaces to the Default group. Only the default group has IP interface.

Group Name	Remove	WAN Interface	LAN Interfaces	DHCP Vendor IDs
Default		ppp0	ENET(1-4) ENET(1-4) wlan0 wl0_Guest1 wl0_Guest2 wl0_Guest3	

To add an Interface Group, click the **Add** button. The following screen will appear. It lists the available and grouped interfaces. Follow the instructions shown below:

Interface grouping Configuration

To create a new interface group:

1. Enter the Group name and the group name must be unique and select either 2. (dynamic) or 3. (static) below:
2. If you like to automatically add LAN clients to a WAN Interface in the new group add the DHCP vendor ID string. By configuring a DHCP vendor ID string any DHCP client request with the specified vendor ID (DHCP option 60) will be denied an IP address from the local DHCP server.
3. Select interfaces from the available interface list and add it to the grouped interface list using the arrow buttons to create the required mapping of the ports. **Note that these clients may obtain public IP addresses**
4. Click Save/Apply button to make the changes effective immediately

IMPORTANT! If a vendor ID is configured for a specific client device, please REBOOT the client device attached to the modem to allow it to obtain an appropriate IP address.

Group Name:

WAN Interface used in the grouping:

Grouped LAN Interfaces

>>

<<

Available LAN Interfaces

ENET(1-4)
eth1
wlan0
wl0_Guest1
wl0_Guest2
wl0_Guest3

Automatically Add Clients With the following DHCP Vendor IDs

Automatically Add Clients with the following DHCP Vendor IDs

Add support to automatically map LAN interfaces to PVC's using DHCP vendor ID (option 60). The local DHCP server will decline and send the requests to a remote DHCP server by mapping the appropriate LAN interface. This will be turned on when Interface Grouping is enabled.

LAN ports

Use this page to enable/disable the Virtual LAN Ports feature

LAN Ports Configuration

Use this page to enable/disable the Virtual LAN Ports feature.

ENET(1-4)

LAN Port
ENET(1-4)
wlan0

Status

Status

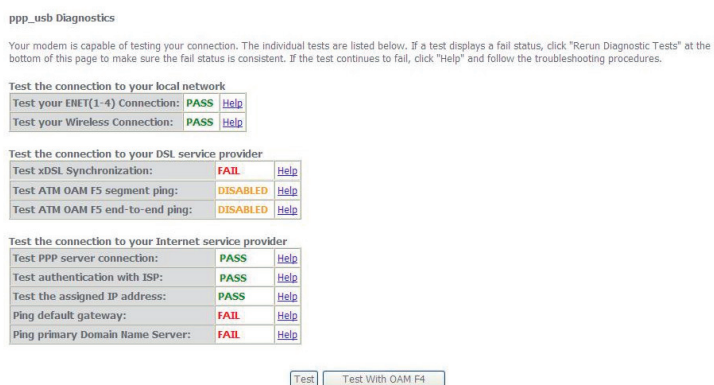
The Status menu has the following submenus:

- Diagnostics
- System Log
- 3G network
- Statistics
- Route
- ARP
- DHCP

Diagnostics

The Diagnostics menu provides feedback on the connection status of the device. The individual tests are listed below. If a test displays a fail status:

- 1: Click on the Help link
- 2: Now click Re-run Diagnostic Tests at the bottom of the screen to re-test and confirm the error
- 3: If the test continues to fail, follow the troubleshooting procedures in the Help screen.



Option	Description
ENET Connection	Pass: Indicates that the Ethernet interface from your computer is connected to the LAN port of this Router. Fail: Indicates that the Router does not detect the Ethernet interface on your computer.
Test your Wireless Connection	Pass: Indicates that the wireless card is ON. Down: Indicates that the wireless card is OFF.
Test xDSL synchronisation	Pass: Indicates that the router has detected an ADSL signal from the telephone company. Fail: Indicates that the router does not detect a signal from the telephone company's DSL network.
Test ATM OAM F5 segment ping	Pass: Indicates that the DSL modem can communicate with the DSL provider network. Fail: Indicates that the DSL modem may not be able to communicate with the DSL provider network. This test may have an effect on your Internet connectivity. Occasionally the DSL provider network may intentionally block this traffic. Therefore if this test fails but you are still able to access the Internet, there is no need to troubleshoot this issue.
Test ATM OAM F5 end-to-end ping	Pass: Indicates that the DSL modem can communicate with the DSL provider network. Fail: Indicates that the DSL modem may not be able to communicate with the DSL provider network. Occasionally the DSL provider network may intentionally block this traffic. Therefore if this test fails but you are still able to access the Internet, there is no need to troubleshoot this issue.
Test PPP server connection	Pass: Indicates that your modem can see the PPP server (the modem received a PADO packet from the PPP server). Fail: Indicates that the modem cannot see the PPP server (the modem did not receive a PADO packet from the PPP server). A flashing green PPP LED on the modem signifies an attempt to establish a PPP connection.
Test authentication with ISP	Pass: Indicates that your username and password stored in the modem has authenticated with ISP's network. Fail: Indicates that the modem was unable to verify your username and password with ISP's network.
Test the assigned IP address	Pass: Indicates that the modem has received a valid IP (Internet Protocol) address from the PPP server. Fail: Indicates that the modem does not have a valid IP address from the PPP server.
Ping default gateway	Pass: Indicates that the modem can communicate with the first entry point to the network. It is usually the IP address of the ISP local router. Fail: Indicates that the modem was unable to communicate with the first entry point on the network. It may not have an effect on your Internet connectivity. Therefore if this test fails but you are still able to access the Internet, there is no need to troubleshoot this issue.
Ping Primary Domain Name Server	Pass: Indicates that the Router can communicate with the primary Domain Name Server (DNS). Fail: Indicates that the Router was unable to communicate with the primary Domain Name Server (DNS). It may not have an effect on your Internet connectivity. Therefore if this test fails but you are still able to access the Internet, there is no need to troubleshoot this issue.

System Log

This function allows you to view system events and configure related options. Follow the steps below to enable and view the System Log.

- 1: Click **Configure System Log** to continue.

System Log

The System Log dialog allows you to view the System Log and configure the System Log options.

Click "View System Log" to view the System Log.

Click "Configure System Log" to configure the System Log options.

View System Log

Configure System Log

- 2: Select the system log options (see table below) and click **Apply/Save**.

System Log -- Configuration

If the log mode is enabled, the system will begin to log all the selected events. For the Log Level, all events above or equal to the selected level will be logged. For the Display Level, all logged events above or equal to the selected level will be displayed. If the selected mode is 'Remote' or 'Both,' events will be sent to the specified IP address and UDP port of the remote syslog server. If the selected mode is 'Local' or 'Both,' events will be recorded in the local memory.

Select the desired values and click 'Apply/Save' to configure the system log options.

Log: Disable Enable

Log Level:

Display Level:

Mode:

Apply/Save

Option	Description
Log	Indicates whether the system is currently recording events. You can enable or disable event logging. By default, it is disabled.
Log level	Allows you to configure the event level and filter out unwanted events below this level. The events ranging from the highest critical level "Emergency" down to this configured level will be recorded to the log buffer on the Router's SDRAM. When the log buffer is full, the newest event will wrap up to the top of the log buffer and overwrite the oldest event. By default, the log level is "Debugging", which is the lowest critical level. The log levels are defined as follows: Emergency is the most serious event level, whereas Debugging is the least important. For instance, if the log level is set to Debugging, all the events from the lowest Debugging level to the most critical level Emergency level will be recorded. If the log level is set to Error, only Error and the level above will be logged.
Display Level	Allows you to select the logged events and displays on the View System Log window for events of this level and above to the highest Emergency level.
Mode	Allows you to specify whether events should be stored in the local memory, be sent to a remote syslog server, or to both simultaneously. If remote mode is selected, the view system log will not be able to display events saved in the remote syslog server. When either Remote mode or Both mode is configured, the WEB UI will prompt the you to enter the Server IP address and Server UDP port.

- 3: Click View System Log. The results are displayed as follows.

System Log

Date/Time	Facility	Severity	Message
Jan 1 00:00:12	kern	crit	kernel: eth0 Link UP.

Refresh

Close

Statistics

These screens provide detailed information for:

- Local Area Network (LAN), Wide Area Network (WAN), ATM and ADSL
- 3G Interfaces

NOTE: These statistics page refresh every 15 seconds.

LAN

This screen displays statistics for the Ethernet and Wireless LAN interfaces

Statistics -- LAN

Interface	Received				Transmitted			
	Bytes	Pkts	Errs	Drops	Bytes	Pkts	Errs	Drops
eth0	3108415	37412	0	0	6705014	10001	0	0
wl0	130825	785	35	0	505295	3042	1654	0

Reset Statistics

Interface	Shows connection interfaces	
Received/Transmitted	Bytes	Rx/TX (receive/transmit) packet in bytes
	Pkts	Rx/TX (receive/transmit) packets
	Errs	Rx/TX (receive/transmit) packets with errors
	Drops	Rx/TX (receive/transmit) packets dropped

WAN

This screen displays statistics for the Ethernet and Wireless LAN interfaces

Statistics -- WAN

Interface	Description	Received				Transmitted			
		Bytes	Pkts	Errs	Drops	Bytes	Pkts	Errs	Drops
ppp0	ppp_usb	0	0	0	0	0	0	0	0

Reset Statistics

Interface	Shows connection interfaces	
Received/Transmitted	Bytes	Rx/TX (receive/transmit) packet in bytes
	Pkts	Rx/TX (receive/transmit) packets
	Errs	Rx/TX (receive/transmit) packets with errors
	Drops	Rx/TX (receive/transmit) packets dropped

ATM

Interface Statistics										
Port Number	In Octets	Out Octets	In Packets	Out Packets	In OAM Cells	Out OAM Cells	In ASM Cells	Out ASM Cells	In Packet Errors	In Cell Errors

Reset

Field	Description
In Octets	Number of received octets over the interface
Out Octets	Number of transmitted octets over the interface
In Errors	Number of cells dropped due to uncorrectable HEC errors
In Unknown	Number of received cells discarded during cell header validation, including cells with unrecognized VPI/VCI values, and cells with invalid cell header patterns. If cells with undefined PTI values are discarded, they are also counted here.
In Hec Errors	Number of cells received with an ATM Cell Header HEX error
In Invalid Vpi Vci Errors	Number of cells received with an unregistered VCC address.
In Port Not Enable Errors	Number of cells received on a port that has not been enabled.
In PTI Errors	Number of cells received with an ATM header Payload Type Indicator (PTI) error
In Idle Cells	Number of idle cells received
In Circuit Type Errors	Number of cells received with an illegal circuit type
In OAM RM CRC Errors	Number of OAM and RM cells received with CRC errors
In GFC Errors	Number of cells received with a non-zero GFC.

ADSL

The following graphic shows the ADSL Network Statistics screen. The Reset button (located at the bottom of the screen) can be used to reset statistics. The bit error rate can be tested by clicking the ADSL BER Test button.

Statistics -- xDSL

Mode:		
Traffic Type:		
Status:	Disabled	
Link Power State:		
	Downstream	Upstream
Line Coding(Trellis):		
SNR Margin (0.1 dB):		
Attenuation (0.1 dB):		
Output Power (0.1 dBm):		
Attainable Rate (Kbps):		
Rate (Kbps):		
Super Frames:		
Super Frame Errors:		
RS Words:		
RS Correctable Errors:		
RS Uncorrectable Errors:		
HEC Errors:		
OCD Errors:		
LCD Errors:		
Total Cells:		
Data Cells:		
Bit Errors:		
Total ES:		
Total SES:		
Total UAS:		

xDSL BER Test

Reset Statistics

Draw Tone Graph

NetComm Gateway Series - ADSL2+/3G Wireless N300 4-Port Modem Router

Consult the table that follows for field descriptions.

Field	Description
Mode	Line Coding format (e.g. G.dmt, G.lite, T1.413, ADSL2)
Type	Channel type (Interleave or Fast)
Line Coding	Trellis On/Off
Status	Lists the status of the ADSL link
Link Power State	Link output power state.
SNR Margin (dB)	Signal to Noise Ratio (SNR) margin
Attenuation (dB)	Estimate of average loop attenuation in the downstream direction.
Output Power (dBm)	Total upstream output power
Attainable Rate (Kbps)	The sync rate you would obtain.
Rate (Kbps)	Current sync rate.

G.DMT mode the following section is inserted here.

K	Number of bytes in DMT frame
R	Number of check bytes in RS code word
S	RS code word size in DMT frame
D	The interleaver depth
Delay	The delay in milliseconds (msec)

In ADSL2+ mode the following section is inserted here.

MSGc	Number of bytes in overhead channel message
B	Number of bytes in Mux Data Frame
M	Number of Mux Data Frames in FEC Data Frame
T	Max Data Frames over sync bytes
R	Number of check bytes in FEC Data Frame
S	Ratio of FEC over PMD Data Frame length
L	Number of bits in PMD Data Frame
D	The interleaver depth
Delay	The delay in milliseconds (msec)

Super Frames	Total number of super frames
Super Frame Errors	Number of super frames received with errors
RS Words	Total number of Reed-Solomon code errors
RS Correctable Errors	Total Number of RS with correctable errors
RS Uncorrectable Errors	Total Number of RS words with uncorrectable errors

HEC Errors	Total Number of Header Error Checksum errors
OCD Errors	Total Number of out-of-cell Delineation errors
LCD Errors	Total number of Loss of Cell Delineation
Total Cells	Total number of ATM cells (including idle and data cells)
Data Cells	Total number of ATM data cells
Bit Errors	Total number of bit errors

In ADSL2+ mode the following section is inserted here.

Total ES:	Total Number of Errored Seconds
Total SES:	Total Number of Severely Errored Seconds
Total UAS:	Total Number of Unavailable Seconds

Route

Select Route to display the paths the Router has found.

Device Info -- Route

Flags: U - up, ! - reject, G - gateway, H - host, R - reinstate
D - dynamic (redirect), M - modified (redirect).

Destination	Gateway	Subnet Mask	Flag	Metric	Service	Interface
192.168.1.0	0.0.0.0	255.255.255.0	U	0		br0

Field	Description
Destination	Destination network or destination host
Gateway	Next hop IP address
Subnet Mask	Subnet Mask of Destination
Flag	U: route is up !: reject route G: use gateway H: target is a host R: reinstate route for dynamic routing D: dynamically installed by daemon or redirect M: modified from routing daemon or redirect
Metric	The 'distance' to the target (usually counted in hops). It is not used by recent kernels, but may be needed by routing daemons.
Service	Shows the name for WAN connection
Interface	Shows connection interfaces

ARP

Click ARP to display the ARP information.

Device Info -- ARP

IP address	Flags	HW Address	Device
192.168.1.2	Complete	00:1E:68:63:4A:45	br0

Field	Description
IP address	Shows IP address of host pc
Flags	Complete Incomplete Permanent Publish
HW Address	Shows the MAC address of host pc
Device	Shows the connection interface

DHCP

Click DHCP to display the DHCP information.

Device Info -- DHCP Leases

Hostname	MAC Address	IP Address	Expires In
Marketing9	00:1e:68:63:4a:45	192.168.1.2	22 hours, 55 minutes, 10 seconds

Field	Description
Hostname	Shows the device/host/PC network name
MAC Address	Shows the Ethernet MAC address of the device/host/PC
IP address	Shows IP address of device/host/PC
Expires In	Shows how much time is left for each DHCP Lease

Appendix

Appendix A: Print Server

These steps explain the procedure for enabling the Print Server.

1. Enable Print Server from the Advanced menu in the Web User Interface.

Select Enable on-board print server checkbox and enter Printer name and Make and model

NOTE: The Printer name can be any text string up to 40 characters. The Make and model can be any text string up to 128 characters.

Print Server settings

This page allows you to enable / disable printer support.

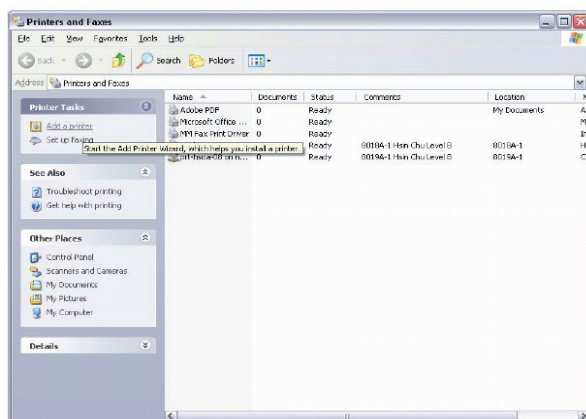
Enable on-board print server.

Printer name

Make and model

For Windows XP:

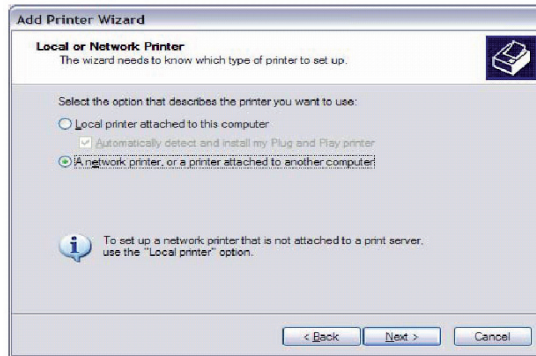
2. Go to the Printers and Faxes application in the Control Panel and select the Add a printer function (as located on the side menu below).



3. Click **Next** to continue, when you see the dialog box below.

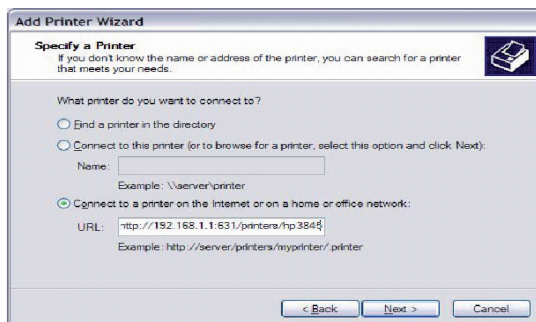


4. Select Network Printer and click **Next**.

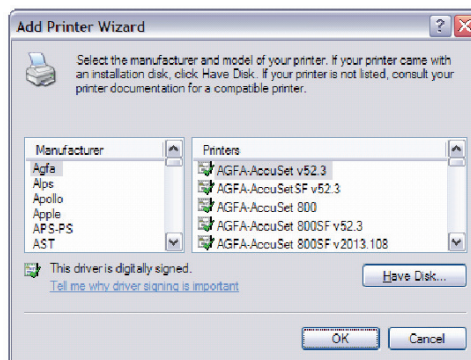


5. Select **Connect** to a printer on the Internet and enter your printer link.
(e.g. <http://192.168.1.1/printers/printername>) and click **Next**.

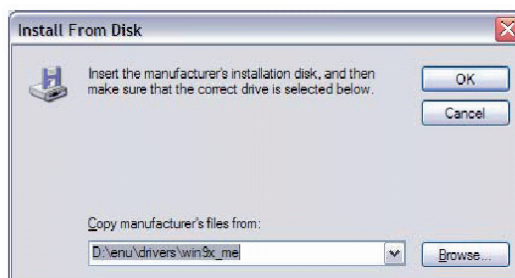
NOTE: The printer name must be the same name entered in the web user interface "printer server setting" as in step 1.



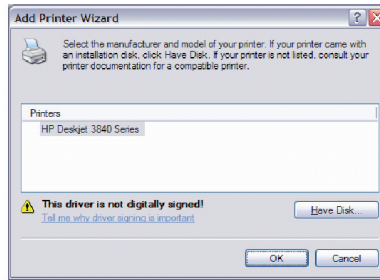
6. Click **Have Disk** and insert the printer driver CD.



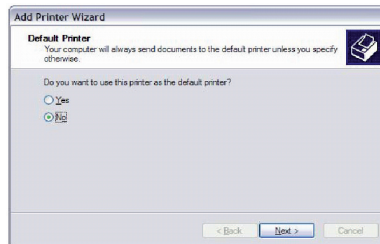
7. Select driver file directory on CD-ROM and click **OK**.



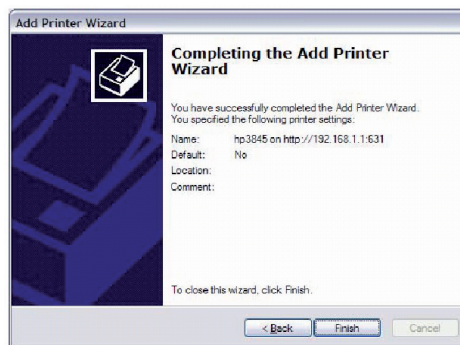
- Once the printer name appears, click **OK**.



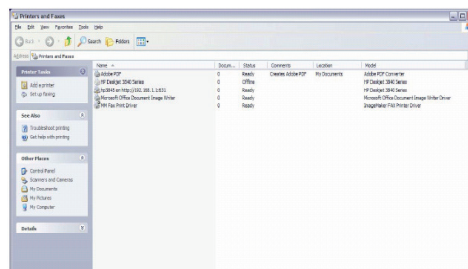
- Choose Yes or No for default printer setting and click **Next**.



- Click **Finish**.



- Check the status of printer from Windows Control Panel, printer window. Status should show as Ready.



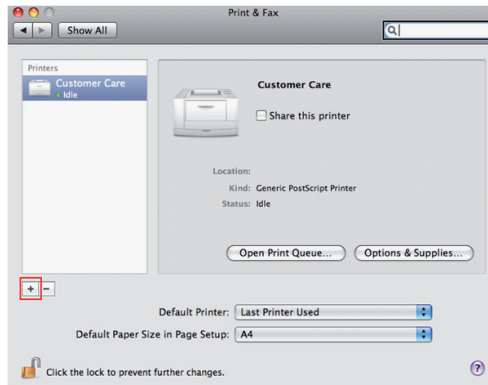
For Mac OSX:

- Browse to the Apple menu and select System Preferences. In the System Preferences menu click on Print & Fax.
- With your Printer driver installed, please add your printer from the Printer & Fax menu.

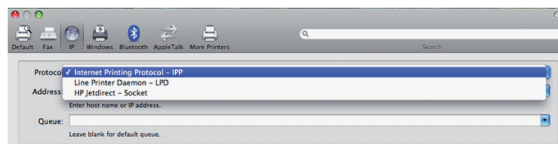


NetComm Gateway Series - ADSL2+/3G Wireless N300 4-Port Modem Router

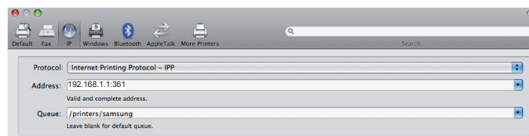
- Click + to add your printer from the Print & Fax menu.



- Select Internet Printing Protocol – IPP from the Protocol drop down list.



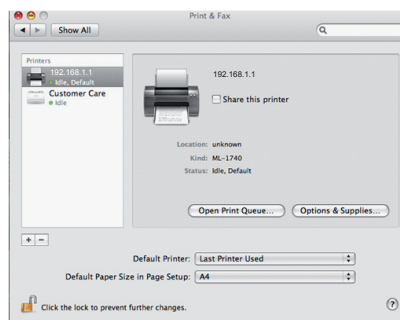
- Type into the Address field “GatewayIPAddress:361” where GatewayIPAddress is the IP address of your Gateway (default: 192.168.1.1). See screenshot below for an example. Also enter into the Queue field “/printers/PrinterName”, where PrinterName is the name you gave your printer in the initial step above.



- Select your printer from the Print Using drop down list.

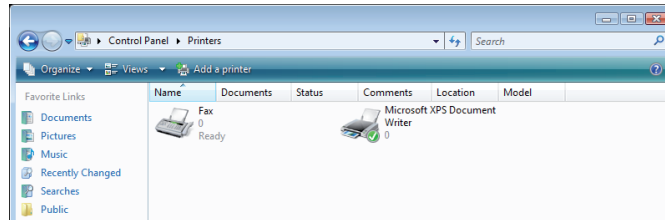


- Click Add and check the printer status.

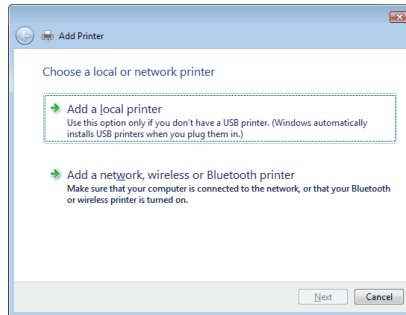


Print Server set up is now complete. You will now be able to print from common applications by selecting this printer from the Print dialogue box.

2. Go to the control panel, and select Printers. Once in the Printers page, click the Add a printer button as shown below.

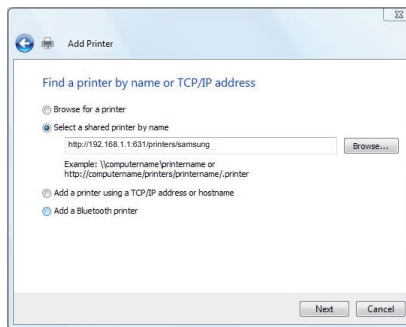


3. Select Add a network, wireless or bluetooth printer.

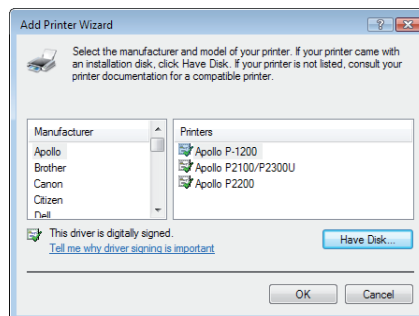


4. Click on the radio-button labelled Select a shared printer by name, and type "http://192.168.1.1/printers/PrinterName" in the box below. Click Next.

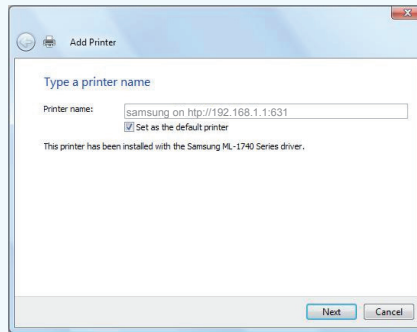
NOTE: The PrinterName must be the same as the printer name entered in the Web User Interface above.



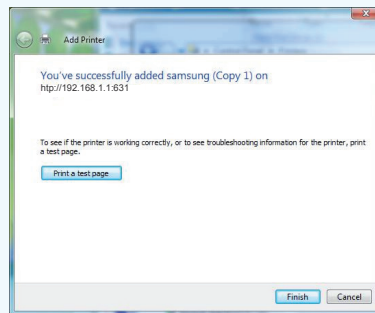
5. Next, select the driver that came with your printer. Browse through the list to select your printer driver, or click 'Have Disk' if you have your printer driver installation media.



6. Choose whether you want this printer to be the default printer, and then click Next.



7. Click Finish. Your device is now configured and ready for use.



Appendix B: USB Storage

These steps explain the procedure for enabling the USB Storage.

1. Enable USB storage from Web User Interface.

Select Enable USB storage checkbox and enter Netbios name and Directory Name

Note: These settings are for advanced users. We recommend that you do not change it if you are unsure of what you are doing. If you do run into problems, you can reset the Gateway back to default settings. To do this, insert a pointed object (like a straightened paperclip) into the hole at the back of the Gateway labelled 'Reset'. Press and hold the reset button till the power light starts flashing - then release the button, you will need to run the Install CD that came in your kit again once you reset the Gateway

Advanced > USB Storage settings

USB Status: **not detected**

This page allows you to enable / disable USB storage .

Enable USB storage

Netbios Name:

Directory Name:

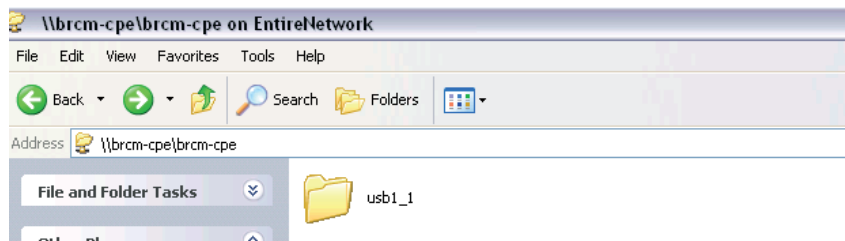
Save/Apply

Field	Description
Netbios Name	It is the hostname of the PC
	The default name is "3G15Wn"
Directory Name	The folder name of "root" directory.
	The default name is "USB-Storage"

For Windows XP:

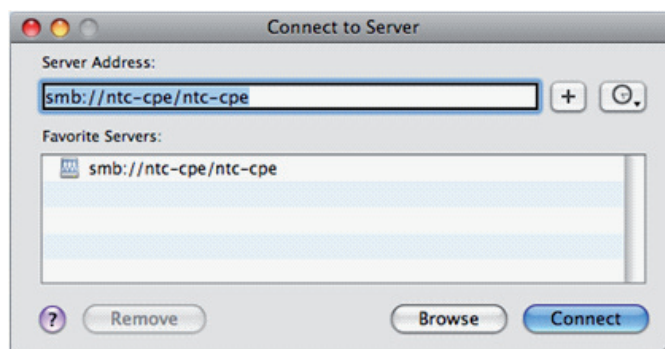
2. Open a web-browser (such as Internet Explorer, Firefox or Safari) and type in the address. \\NetbiosName\DirectoryName\ (eg. \\3G15Wn\USB-Storage)

Note: There is no username and password required to access the USB drive, the user will be able to read/write the folder/files in the USB drive.

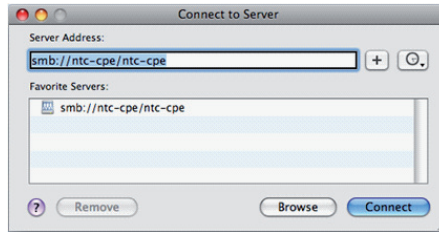


For Mac OSX:

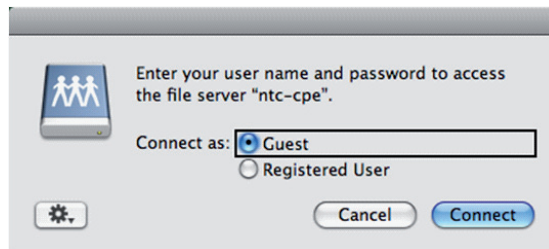
2. From the Finder, select the Go and then click Connect to Server
3. In the address field of the Connect to Server dialog, type in the address: smb:// "NetbiosName"/"DirectoryName" (eg smb://3G15Wn/USB-Storage)



4. Click the + button to add this server to the list of Favourites and then click Connect

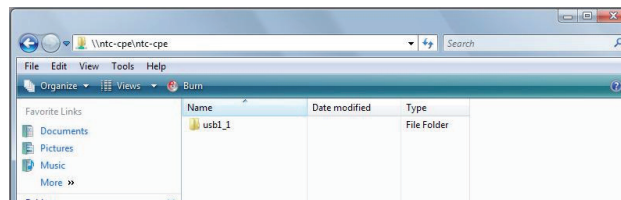


5. Select the Guest radio button and then click Connect



For Windows Vista

1. Open a web-browser (such as Internet Explorer, Firefox or Safari)
2. Type in the address “\\NetbiosName\DirectoryName\” (eg \\3G15Wn\USB-Storage)



Note: There is no username and password required to access the USB drive. Any network user will be able to read/write the folder/files in the USB drive.

Legal & Regulatory Information

This manual is copyright. Apart from any fair dealing for the purposes of private study, research, criticism or review, as permitted under the Copyright Act, no part may be reproduced, stored in a retrieval system or transmitted in any form, by any means, be it electronic, mechanical, recording or otherwise, without the prior written permission of NetComm Limited. NetComm Limited accepts no liability or responsibility, for consequences arising from the use of this product.

NetComm Limited reserves the right to change the specifications and operating details of this product without notice.

NetComm is a registered trademark of NetComm Limited.

All other trademarks are acknowledged the property of their respective owners.

Customer Information

ACA (Australian Communications Authority) requires you to be aware of the following information and warnings:

- (1) This unit shall be connected to the Telecommunication Network through a line cord which meets the requirements of the ACA TS008 Standard.
- (2) This equipment has been tested and found to comply with the Standards for C-Tick and or A-Tick as set by the ACA . These standards are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio noise and, if not installed and used in accordance with the instructions detailed within this manual, may cause interference to radio communications. However, there is no guarantee that interference will not occur with the installation of this product in your home or office. If this equipment does cause some degree of interference to radio or television reception, which can be determined by turning the equipment off and on, we encourage the user to try to correct the interference by one or more of the following measures:
 - Change the direction or relocate the receiving antenna.
 - Increase the separation between this equipment and the receiver.
 - Connect the equipment to an alternate power outlet on a different power circuit from that to which the receiver/TV is connected.
 - Consult an experienced radio/TV technician for help.
- (3) The power supply that is provided with this unit is only intended for use with this product. Do not use this power supply with any other product or do not use any other power supply that is not approved for use with this product by NetComm. Failure to do so may cause damage to this product, fire or result in personal injury.

Product Warranty

The warranty is granted on the following conditions:

1. This warranty extends to the original purchaser (you) and is not transferable;
2. This warranty shall not apply to software programs, batteries, power supplies, cables or other accessories supplied in or with the product;
3. The customer complies with all of the terms of any relevant agreement with NetComm and any other reasonable requirements of NetComm including producing such evidence of purchase as NetComm may require;
4. The cost of transporting product to and from NetComm's nominated premises is your responsibility; and,
5. NetComm does not have any liability or responsibility under this warranty where any cost, loss, injury or damage of any kind, whether direct, indirect, consequential, incidental or otherwise arises out of events beyond NetComm's reasonable control. This includes but is not limited to: acts of God, war, riot, embargoes, acts of civil or military authorities, fire, floods, electricity outages, lightning, power surges, or shortages of materials or labour.
6. The customer is responsible for the security of their computer and network at all times. Security features may be disabled within the factory default settings. NetComm recommends that you enable these features to enhance your security.

GNU General Public License

This product includes software code that is subject to the GNU General Public License ("GPL") or GNU Lesser General Public License ("LGPL"). This code is subject to the copyrights of one or more authors and is distributed without any warranty. A copy of this software can be obtained by contacting NetComm Limited on +61 2 9424 2059.

The warranty is automatically voided if:

1. You, or someone else, use the product, or attempts to use it, other than as specified by NetComm;
2. The fault or defect in your product is the result of a voltage surge subjected to the product either by the way of power supply or communication line, whether caused by thunderstorm activity or any other cause(s);
3. The fault is the result of accidental damage or damage in transit, including but not limited to liquid spillage;
4. Your product has been used for any purposes other than that for which it is sold, or in any way other than in strict accordance with the user manual supplied;
5. Your product has been repaired or modified or attempted to be repaired or modified, other than by a qualified person at a service centre authorised by NetComm; and,
6. The serial number has been defaced or altered in any way or if the serial number plate has been removed.

Limitations of Warranty

The Trade Practices Act 1974 and corresponding State and Territory Fair Trading Acts or legalisation of another Government (“the relevant acts”) in certain circumstances imply mandatory conditions and warranties which cannot be excluded. This warranty is in addition to and not in replacement for such conditions and warranties.

To the extent permitted by the Relevant Acts, in relation to your product and any other materials provided with the product (“the Goods”) the liability of NetComm under the Relevant Acts is limited at the option of NetComm to:

- Replacement of the Goods; or
- Repair of the Goods; or
- Payment of the cost of replacing the Goods; or
- Payment of the cost of having the Goods repaired.

All NetComm ACN 002 490 486 products have a standard 12 months warranty from date of purchase. However some products have an extended warranty option (refer to packaging). To be eligible for the extended warranty you must supply the requested warranty information to NetComm within 30 days of the original purchase by registering on-line via the NetComm web site at

www.netcomm.com.au

Product Warranty

NetComm products have a standard 12 months warranty from date of purchase. However some products have an extended warranty option, via registering your product online at the NetComm website www.netcomm.com.au.

Technical Support

If you have any technical difficulties with your product, please refer to the support section of our website.

www.netcomm.com.au/support

Note: NetComm Technical Support for this product only covers the basic installation and features outlined in the Quick Start Guide. For further information regarding the advanced features of this product, please refer to the configuring sections in the User Guide or contact a Network Specialist.



NETCOMM LIMITED PO Box 1200, Lane Cove NSW 2066 Australia
P: 02 9424 2070 **F:** 02 9424 2010
E: sales@netcomm.com.au **W:** www.netcomm.com.au

DYNALINK NZ 12c Tea Kea Place, Albany, Auckland, New Zealand
P: 09 448 5548 **F:** 09 448 5549
E: sales@dynalink.co.nz **W:** www.dynalink.co.nz

Trademarks and registered trademarks are the property of NetComm Limited or their respective owners.
Specifications are subject to change without notice. Images shown may vary slightly from the actual product.